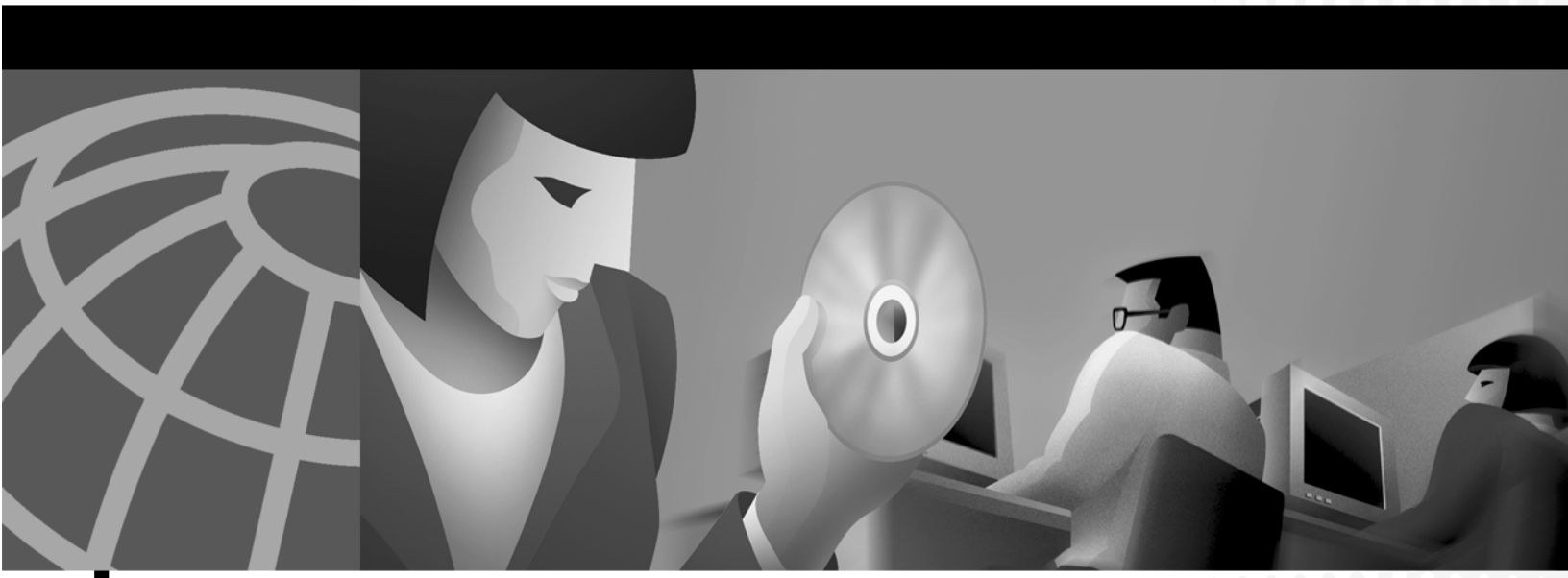


Cisco Secure ACS 3.0 for Windows 2000/NT Servers User Guide

November 2001

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7813751=
Text Part Number: 78-13751-01

Downloaded from www.Manualslib.com manuals search engine

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

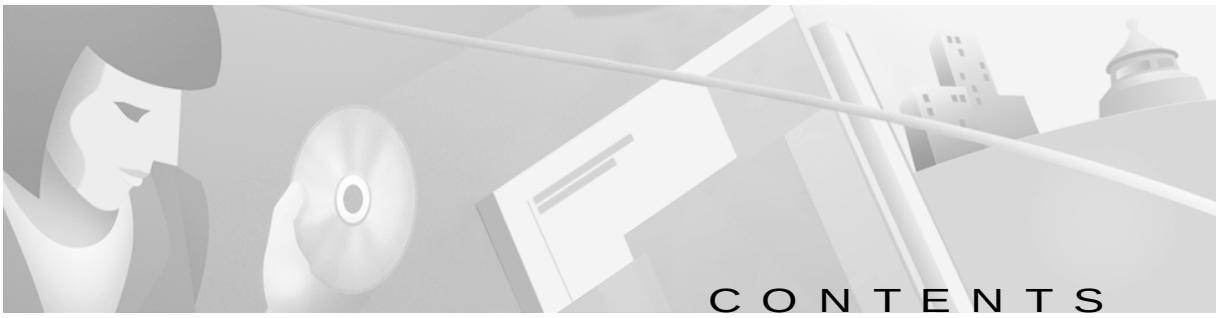
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That's Possible are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0110R)

Cisco Secure ACS 3.0 for Windows 2000/NT Servers User Guide
Copyright © 2001, Cisco Systems, Inc.
All rights reserved

Downloaded from www.Manualslib.com manuals search engine



CONTENTS

Preface xxvii

Document Objectives **xxvii**

Who Should Read This Guide **xxvii**

How This Guide is Organized **xxviii**

Conventions Used in This Guide **xxx**

Related Documentation **xxxi**

Obtaining Documentation **xxxii**

World Wide Web **xxxii**

Documentation CD-ROM **xxxii**

Ordering Documentation **xxxii**

Documentation Feedback **xxxiii**

Obtaining Technical Assistance **xxxiii**

Cisco.com **xxxiii**

Technical Assistance Center **xxxiv**

Cisco TAC Web Site **xxxiv**

Cisco TAC Escalation Center **xxxv**

CHAPTER 1 **Overview of Cisco Secure ACS 1-1**

The Cisco Secure ACS Paradigm **1-1**

Cisco Secure ACS Specifications **1-2**

System Performance Specifications **1-3**

Cisco Secure ACS Windows Services **1-3**

Downloaded from www.Manualslib.com manuals search engine

AAA Server Functions and Concepts **1-4**
Cisco Secure ACS and the AAA Client **1-5**
AAA Protocols—TACACS+ and RADIUS **1-5**
TACACS+ **1-6**
RADIUS **1-6**
Authentication **1-7**
Authentication Considerations **1-8**
Authentication and User Databases **1-8**
Passwords **1-10**
Other Authentication-Related Features **1-14**
Authorization **1-15**
Max Sessions **1-16**
Dynamic Usage Quotas **1-16**
Other Authorization-Related Features **1-17**
Accounting **1-17**
Other Accounting-Related Features **1-18**
Administration **1-18**
HTTP Port Allocation for Remote Administrative Sessions **1-19**
Network Device Groups **1-20**
Other Administration-Related Features **1-20**
Cisco Secure ACS HTML Interface **1-21**
About the Cisco Secure ACS HTML Interface **1-21**
HTML Interface Layout **1-22**
Uniform Resource Locator for the HTML Interface **1-24**
Network Environments and Remote Administrative Sessions **1-24**
Remote Administrative Sessions and HTTP Proxy **1-24**
Remote Administrative Sessions through Firewalls **1-25**

Downloaded from www.Manualslib.com manuals search engine

Remote Administrative Sessions through a NAT Gateway **1-25**
Accessing the HTML Interface **1-26**
Logging Off the HTML Interface **1-26**
Online Help and Online Documentation **1-27**
Using Online Help **1-27**
Using the Online Documentation **1-28**

CHAPTER 2 **Deploying Cisco Secure ACS 2-1**
Basic Deployment Requirements for Cisco Secure ACS **2-2**
System Requirements **2-2**
Hardware Requirements **2-2**
Operating System Requirements **2-3**
Third-Party Software Requirements **2-3**
Network Requirements **2-4**
Basic Deployment Factors for Cisco Secure ACS **2-4**
Network Topology **2-5**
Dial-Up Topology **2-5**
Wireless Network **2-8**
Remote Access using VPN **2-11**
Remote Access Policy **2-13**
Security Policy **2-14**
Administrative Access Policy **2-14**
Separation of Administrative and General Users **2-16**
Database **2-17**
Number of Users **2-17**
Type of Database **2-17**

Downloaded from www.Manualslib.com manuals search engine

Network Speed and Reliability 2-18
Suggested Deployment Sequence 2-18

CHAPTER 3 **Setting Up the Cisco Secure ACS HTML Interface 3-1**
Interface Design Concepts 3-2
User-to-Group Relationship 3-2
Per-User or Per-Group Features 3-2
User Data Configuration Options 3-3
Defining New User Data Fields 3-3
Advanced Options 3-4
Setting Advanced Options for the Cisco Secure ACS User Interface 3-6
Protocol Configuration Options for TACACS+ 3-7
Setting Options for TACACS+ 3-9
Protocol Configuration Options for RADIUS 3-10
Setting Protocol Configuration Options for (IETF) RADIUS 3-12
Setting Protocol Configuration Options for RADIUS (Cisco IOS/PIX) 3-14
Setting Protocol Configuration Options for RADIUS (Ascend) 3-14
Setting Protocol Configuration Options for RADIUS (Cisco VPN 3000) 3-15
Setting Protocol Configuration Options for RADIUS (Cisco VPN 5000) 3-16
Setting Protocol Configuration Options for RADIUS (Microsoft) 3-17
Setting Protocol Configuration Options for RADIUS (Nortel) 3-18
Setting Protocol Configuration Options for RADIUS (Juniper) 3-19
Setting Protocol Configuration Options for RADIUS (Cisco BBSM) 3-20

CHAPTER 4 **Setting Up and Managing Network Configuration 4-1**
About Distributed Systems 4-2
AAA Servers in Distributed Systems 4-3

Downloaded from www.Manualslib.com manuals search engine

Default Distributed System Settings 4-3
Proxy in Distributed Systems 4-4
Fallback on Failed Connection 4-5
Character String 4-6
Stripping 4-6
Proxy in an Enterprise 4-6
Remote Use of Accounting Packets 4-7
Other Features Enabled by System Distribution 4-8
AAA Client Configuration 4-8
Adding and Configuring a AAA Client 4-9
Editing an Existing AAA Client 4-12
Deleting a AAA Client 4-14
AAA Server Configuration 4-15
Adding and Configuring a AAA Server 4-16
Editing a AAA Server Configuration 4-18
Deleting a AAA Server 4-20
Network Device Group Configuration 4-20
Adding a Network Device Group 4-21
Assigning an Unassigned AAA Client or AAA Server to an NDG 4-22
Reassigning a AAA Client or AAA Server to an NDG 4-23
Renaming a Network Device Group 4-23
Deleting a Network Device Group 4-24
Proxy Distribution Table Configuration 4-25
About the Proxy Distribution Table 4-25
Adding a New Proxy Distribution Table Entry 4-26
Sorting the Character String Match Order of Distribution Entries 4-28

Downloaded from www.Manualslib.com manuals search engine

Editing a Proxy Distribution Table Entry 4-28
Deleting a Proxy Distribution Table Entry 4-29

CHAPTER 5 **Setting Up and Managing Shared Profile Components 5-1**
Downloadable PIX ACLs 5-2
About Downloadable PIX ACLs 5-2
Downloadable PIX ACL Configuration 5-3
Adding a Downloadable PIX ACL 5-3
Editing a Downloadable PIX ACL 5-4
Deleting a Downloadable PIX ACL 5-5
Network Access Restrictions 5-6
About Network Access Restrictions 5-6
Shared Network Access Restrictions Configuration 5-7
Adding a Shared Network Access Restriction 5-8
Editing a Shared Network Access Restriction 5-10
Deleting a Shared Network Access Restriction 5-12
Command Authorization Sets 5-12
About Command Authorization Sets 5-13
About Pattern Matching 5-14
Command Authorization Sets Configuration 5-14
Adding a Command Authorization Set 5-15
Editing a Command Authorization Set 5-17
Deleting a Command Authorization Set 5-17

CHAPTER 6 **Setting Up and Managing User Groups 6-1**
User Group Setup Features and Functions 6-2
Default Group 6-2

Downloaded from www.Manualslib.com manuals search engine

Group TACACS+ Settings 6-2
Common User Group Settings 6-3
Enabling VoIP Support for a User Group 6-4
Setting Default Time of Day Access for a User Group 6-5
Setting Callback Options for a User Group 6-6
Setting Network Access Restrictions for a User Group 6-7
Setting Max Sessions for a User Group 6-11
Setting Usage Quotas for a User Group 6-13
Configuration-specific User Group Settings 6-15
Setting Token Card Settings for a User Group 6-17
Setting Enable Privilege Options for a User Group 6-18
Enabling Password Aging for the CiscoSecure User Database 6-20
Varieties of Password Aging Supported by Cisco Secure ACS 6-20
Password Aging Feature Settings 6-21
Enabling Password Aging for Users in Windows Databases 6-25
Setting IP Address Assignment Method for a User Group 6-26
Assigning a Downloadable PIX ACL to a Group 6-27
Configuring TACACS+ Settings for a User Group 6-28
Configuring a Shell Command Authorization Set for a User Group 6-30
Configuring a PIX Command Authorization Set for a User Group 6-32
Configuring IETF RADIUS Settings for a User Group 6-34
Configuring Cisco IOS/PIX RADIUS Settings for a User Group 6-36
Configuring Ascend RADIUS Settings for a User Group 6-37
Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group 6-38
Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group 6-39

Downloaded from www.Manualslib.com manuals search engine

Configuring Microsoft RADIUS Settings for a User Group 6-41
Configuring Nortel RADIUS Settings for a User Group 6-42
Configuring Juniper RADIUS Settings for a User Group 6-44
Configuring Cisco BBSM RADIUS Settings for a User Group 6-45
Configuring Custom RADIUS VSA Settings for a User Group 6-46
Group Setting Management 6-48
Listing Users in a User Group 6-48
Resetting Usage Quota Counters for a User Group 6-49
Renaming a User Group 6-49
Saving Changes to User Group Settings 6-50

CHAPTER 7 **Setting Up and Managing User Accounts 7-1**
User Setup Features and Functions 7-2
About User Databases 7-3
Basic User Setup Options 7-4
Adding a Basic User Account 7-5
Setting Supplementary User Information 7-7
Setting a Separate CHAP/MS-CHAP/ARAP Password 7-8
Assigning a User to a Group 7-9
Setting User Callback Option 7-10
Assigning a User to a Client IP Address 7-11
Setting Network Access Restrictions for a User 7-12
Setting Max Sessions Options for a User 7-17
Setting User Usage Quotas Options 7-19
Setting Options for User Account Disablement 7-21
Assigning a PIX ACL to a User 7-22

Downloaded from www.Manualslib.com manuals search engine

Advanced User Authentication Settings **7-23**
TACACS+ Settings (User) **7-24**
Configuring TACACS+ Settings for a User **7-24**
Configuring a Shell Command Authorization Set for a User **7-26**
Configuring a PIX Command Authorization Set for a User **7-29**
Configuring the Unknown Service Setting for a User **7-31**
Advanced TACACS+ Settings (User) **7-31**
Setting Enable Privilege Options for a User **7-32**
Setting TACACS+ Enable Password Options for a User **7-34**
Setting TACACS+ Outbound Password for a User **7-35**
RADIUS Attributes **7-36**
Setting IETF RADIUS Parameters for a User **7-37**
Setting Cisco IOS/PIX RADIUS Parameters for a User **7-38**
Setting Ascend RADIUS Parameters for a User **7-39**
Setting Cisco VPN 3000 Concentrator RADIUS Parameters for a User **7-41**
Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User **7-42**
Setting Microsoft RADIUS Parameters for a User **7-44**
Setting Nortel RADIUS Parameters for a User **7-45**
Setting Juniper RADIUS Parameters for a User **7-47**
Setting BBSM RADIUS Parameters for a User **7-48**
Setting Custom RADIUS Attributes for a User **7-49**
User Management **7-51**
Listing All Users **7-51**
Finding a User **7-52**
Disabling a User Account **7-53**

Downloaded from www.Manualslib.com manuals search engine

Deleting a User Account 7-54
Resetting User Session Quota Counters 7-55
Resetting a User Account after Login Failure 7-55
Saving User Settings 7-56

CHAPTER 8 **Establishing Cisco Secure ACS System Configuration** 8-1
Service Control 8-2
Determining the Status of Cisco Secure ACS Services 8-2
Stopping, Starting, or Restarting Services 8-2
Logging 8-3
Date Format Control 8-3
Setting the Date Format 8-4
Password Validation 8-4
Setting Password Validation Options 8-5
CiscoSecure Database Replication 8-6
About CiscoSecure Database Replication 8-6
Replication Process 8-8
Replication Frequency 8-10
Important Implementation Considerations 8-10
Database Replication Versus Database Backup 8-11
Database Replication Logging 8-12
Replication Options 8-13
Replication Components Options 8-13
Replication Scheduling Options 8-14
Replication Partners Options 8-15
Implementing Primary and Secondary Replication Setups on Cisco Secure ACS Servers 8-16

Downloaded from www.Manualslib.com manuals search engine

Configuring a Secondary Cisco Secure ACS Server 8-17
Replicating Immediately 8-18
Scheduling Replication 8-20
Disabling CiscoSecure Database Replication 8-23
Database Replication Event Error Alert Notification 8-23
RDBMS Synchronization 8-24
About RDBMS Synchronization 8-24
RDBMS Synchronization Components 8-25
About CSDBSync 8-25
About the accountActions Table 8-26
Cisco Secure ACS Database Recovery Using the accountActions Table 8-28
Reports and Event (Error) Handling 8-29
Preparing to Use RDBMS Synchronization 8-29
Considerations for Using CSV-Based Synchronization 8-30
Preparing for CSV-Based Synchronization 8-31
Configuring a System Data Source Name for RDBMS Synchronization 8-32
RDBMS Synchronization Options 8-33
RDBMS Setup Options 8-34
Synchronization Scheduling Options 8-34
Synchronization Partners Options 8-35
Performing RDBMS Synchronization Immediately 8-35
Scheduling RDBMS Synchronization 8-37
Disabling Scheduled RDBMS Synchronizations 8-39
Cisco Secure ACS Backup 8-40
About Cisco Secure ACS Backup 8-40
Backup File Locations 8-41
Directory Management 8-41

Downloaded from www.Manualslib.com manuals search engine

Components Backed Up 8-41
Reports of Cisco Secure ACS Backups 8-42
Performing a Manual Cisco Secure ACS Backup 8-42
Scheduling Cisco Secure ACS Backups 8-43
Disabling Scheduled Cisco Secure ACS Backups 8-44
Cisco Secure ACS System Restore 8-45
About Cisco Secure ACS System Restore 8-45
Backup File Names and Locations 8-45
Components Restored 8-47
Reports of Cisco Secure ACS Restorations 8-47
Restoring Cisco Secure ACS from a Backup File 8-47
Cisco Secure ACS Active Service Management 8-48
System Monitoring 8-49
System Monitoring Options 8-49
Setting Up System Monitoring 8-50
Event Logging 8-51
Setting Up Event Logging 8-51
IP Pools Server 8-52
Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges 8-53
Refreshing the AAA Server IP Pools Table 8-55
Adding a New IP Pool 8-55
Editing an IP Pool Definition 8-56
Resetting an IP Pool 8-57
Deleting an IP Pool 8-58
IP Pools Address Recovery 8-59
Enabling IP Pool Address Recovery 8-59

Downloaded from www.Manualslib.com manuals search engine

VoIP Accounting Configuration **8-60**
Configuring VoIP Accounting **8-61**
Cisco Secure ACS Certificate Setup **8-61**
Background on Certification **8-62**
EAP-TLS Setup Overview **8-63**
Requirements for Certificate Enrollment **8-63**
Generating a Request for a Certificate **8-64**
Installing Cisco Secure ACS Certification with Manual Enrollment **8-66**
Installing Cisco Secure ACS Certification with Automatic Enrollment **8-68**
Performing Cisco Secure ACS Certification Update or Replacement **8-69**
Certification Authority Setup **8-70**
Trust Requirements and Models **8-71**
Editing the Certificate Trust List **8-72**
Adding a New CA Certificate to Local Certificate Storage **8-72**
Global Authentication Setup **8-73**

CHAPTER 9 **Working with Logging and Reports** **9-1**
Logging Formats **9-1**
Special Logging Attributes **9-2**
Update Packets In Accounting Logs **9-3**
About Cisco Secure ACS Logs and Reports **9-4**
Accounting Logs **9-4**
TACACS+ Accounting Log **9-5**
TACACS+ Administration Log **9-6**
RADIUS Accounting Log **9-7**
VoIP Accounting Log **9-8**
Failed Attempts Log **9-9**

Downloaded from www.Manualslib.com manuals search engine

Passed Authentications Log 9-10
Dynamic Cisco Secure ACS Administration Reports 9-10
Logged-In Users Report 9-11
Disabled Accounts Report 9-14
Cisco Secure ACS System Logs 9-15
ACS Backup and Restore Log 9-15
RDBMS Synchronization Log 9-16
Database Replication Log 9-16
Administration Audit Log 9-17
ACS Service Monitoring Log 9-18
Working with CSV Logs 9-19
CSV Log File Names 9-19
Enabling or Disabling a CSV Log 9-19
Viewing a CSV Report 9-20
Configuring a CSV Log 9-22
Working with ODBC Logs 9-25
Preparing to Use ODBC Logging 9-25
Configuring a System Data Source Name for ODBC Logging 9-26
Configuring an ODBC Log 9-27
Remote Logging 9-29
About Remote Logging 9-30
Remote Logging Options 9-31
Configuring a Central Logging Server 9-31
Enabling and Configuring Remote Logging 9-32
Disabling Remote Logging 9-33

Downloaded from www.Manualslib.com manuals search engine

Service Logs **9-34**

Services Logged **9-34**

Configuring Service Logs **9-35**

CHAPTER 10 **Setting Up and Managing Administrators and Policy 10-1**

Administrator Accounts **10-1**

Administrator Privileges **10-2**

Adding an Administrator Account **10-6**

Editing an Administrator Account **10-7**

Deleting an Administrator Account **10-9**

Access Policy **10-10**

Access Policy Options **10-10**

Setting Up Access Policy **10-12**

Session Policy **10-13**

Session Policy Options **10-13**

Setting Up Session Policy **10-14**

Audit Policy **10-16**

CHAPTER 11 **Working with User Databases 11-1**

CiscoSecure User Database **11-2**

About External User Databases **11-4**

Authenticating with External User Databases **11-5**

Windows NT/2000 User Database **11-6**

The Cisco Secure ACS Authentication Process with Windows NT/2000 User Databases **11-7**

Trust Relationships **11-8**

Downloaded from www.Manualslib.com manuals search engine

Windows Dial-up Networking Clients **11-9**

About the Windows NT/2000 Dial-up Networking Client **11-9**

About the Windows 95/98/Millennium Edition Dial-up Networking Client **11-10**

Windows NT/2000 Authentication **11-10**

User-Changeable Passwords with Windows NT/2000 User Databases **11-12**

Preparing Users for Authenticating with Windows NT/2000 **11-12**

Configuring a Windows NT/2000 External User Database **11-13**

Generic LDAP **11-14**

Cisco Secure ACS Authentication Process with a Generic LDAP User Database **11-15**

Multiple LDAP Instances **11-16**

LDAP Organizational Units and Groups **11-17**

Directed Authentications **11-17**

LDAP Failover **11-17**

Successful Previous Authentication with the Primary LDAP Server **11-18**

Unsuccessful Previous Authentication with the Primary LDAP Server **11-18**

Configuring a Generic LDAP External User Database **11-19**

Novell NDS Database **11-24**

User Contexts **11-25**

Novell NDS External User Database Options **11-27**

Configuring a Novell NDS External User Database **11-28**

ODBC Database **11-30**

Cisco Secure ACS Authentication Process with an ODBC External User Database **11-31**

Preparing to Authenticate Users with an ODBC-Compliant Relational Database **11-32**

Downloaded from www.Manualslib.com manuals search engine

Implementation of Stored Procedures for ODBC Authentication **11-33**

Type Definitions **11-34**

Microsoft SQL Server and Case-Sensitive Passwords **11-34**

Sample Routine for Generating a PAP Authentication SQL Procedure **11-35**

Sample Routine for Generating an SQL CHAP Authentication Procedure **11-36**

PAP Authentication Procedure Input **11-36**

PAP Procedure Output **11-37**

CHAP/MS-CHAP/ARAP Authentication Procedure Input **11-38**

CHAP/MS-CHAP/ARAP Procedure Output **11-38**

Result Codes **11-39**

Configuring a System Data Source Name for an ODBC External User Database **11-40**

Configuring an ODBC External User Database **11-41**

LEAP Proxy RADIUS Server Database **11-44**

Configuring a LEAP Proxy RADIUS Server External User Database **11-45**

Token Server User Databases **11-47**

About Token Servers and Cisco Secure ACS **11-48**

Token Servers and ISDN **11-48**

RADIUS-Enabled Token Servers **11-49**

About RADIUS-Enabled Token Servers **11-49**

Token Server RADIUS Authentication Request and Response Contents **11-50**

Configuring a RADIUS Token Server External User Database **11-50**

Token Servers with Vendor-Proprietary Interfaces **11-53**

About Token Servers with Proprietary Interfaces **11-53**

Configuring a SafeWord Token Server External User Database **11-53**

Downloaded from www.Manualslib.com manuals search engine

Configuring an AXENT Token Server External User Database
AXENT **11-55**

Configuring an RSA SecurID Token Server External User Database **11-56**

Deleting an External User Database Configuration **11-58**

CHAPTER 12 **Administering External User Databases 12-1**

Unknown User Processing **12-1**

Known, Unknown, and Cached Users **12-2**

General Authentication Request Handling and Rejection Mode **12-3**

Authentication Request Handling and Rejection Mode with the Windows NT/2000 User Database **12-4**

Windows Authentication with a Domain Specified **12-4**

Windows Authentication with Domain Omitted **12-5**

Performance of Unknown User Authentication **12-6**

Added Latency **12-6**

Authentication Timeout Value on AAA clients **12-6**

Network Access Authorization **12-7**

Unknown User Policy **12-7**

Database Search Order **12-8**

Configuring the Unknown User Policy **12-8**

Turning off External User Database Authentication **12-9**

Database Group Mappings **12-10**

Group Mapping by External User Database **12-10**

Creating a Cisco Secure ACS Group Mapping for a Token Server, ODBC Database, or LEAP Proxy RADIUS Server Database **12-12**

Group Mapping by Group Set Membership **12-13**

Group Mapping Order **12-13**

No Access Group for Group Set Mappings **12-14**

Downloaded from www.Manualslib.com manuals search engine

Default Group Mapping for Windows NT/2000 **12-14**

Creating a Cisco Secure ACS Group Mapping for Windows NT/2000, Novell NDS, or Generic LDAP Groups **12-15**

Editing a Windows NT/2000, Novell NDS, or Generic LDAP Group Set Mapping **12-17**

Deleting a Windows NT/2000, Novell NDS, or Generic LDAP Group Set Mapping **12-18**

Deleting a Windows NT/2000 Domain Group Mapping Configuration **12-19**

Changing Group Set Mapping Order **12-20**

RADIUS-Based Group Specification **12-21**

APPENDIX A **Troubleshooting Information for Cisco Secure ACS A-1**

Administration Issues **A-2**

Browser Issues **A-3**

Cisco IOS Issues **A-4**

Database Issues **A-5**

Dial-in Connection Issues **A-6**

Debug Issues **A-11**

Proxy Issues **A-12**

Installation and Upgrade Issues **A-13**

MaxSessions Issues **A-13**

Report Issues **A-14**

Third-Party Server Issues **A-15**

PIX Firewall Issues **A-16**

User Authentication Issues **A-16**

TACACS+ and RADIUS Attribute Issues **A-18**

Downloaded from www.Manualslib.com manuals search engine

APPENDIX B **System Messages B-1**

Windows NT/2000 Event Log Service Startup Errors **B-1**

System Monitored Events **B-2**

Replication Messages **B-6**

Failed Attempts Messages **B-9**

APPENDIX C **TACACS+ Attribute-Value Pairs C-1**

Cisco IOS Attribute-Value Pair Dictionary **C-1**

TACACS+ AV Pairs **C-2**

TACACS+ Accounting AV Pairs **C-4**

APPENDIX D **RADIUS Attributes D-1**

Cisco IOS Dictionary of RADIUS AV Pairs **D-2**

Cisco IOS/PIX Dictionary of RADIUS VSAs **D-4**

Cisco VPN 3000 Concentrator Dictionary of RADIUS VSAs **D-6**

Cisco VPN 5000 Concentrator Dictionary of RADIUS VSAs **D-9**

Cisco Building Broadband Service Manager Dictionary of RADIUS VSA **D-9**

Vendor-Proprietary IETF RADIUS AV Pairs **D-10**

IETF Dictionary of RADIUS AV Pairs **D-12**

RADIUS (IETF) Accounting AV Pairs **D-16**

Microsoft MPPE Dictionary of RADIUS VSAs **D-18**

Ascend Dictionary of RADIUS AV Pairs **D-21**

Nortel Dictionary of RADIUS VSAs **D-29**

Juniper Dictionary of RADIUS VSAs **D-30**

Downloaded from www.Manualslib.com manuals search engine

APPENDIX E **Cisco Secure ACS Command-Line Database Utility** **E-1**

Location of CSUtil.exe and Related Files **E-2**

CSUtil.exe Syntax **E-2**

CSUtil.exe Options **E-3**

Backing Up Cisco Secure ACS with CSUtil.exe **E-5**

Restoring Cisco Secure ACS with CSUtil.exe **E-6**

Creating a CiscoSecure User Database **E-7**

Creating a Cisco Secure ACS Database Dump File **E-9**

Loading the Cisco Secure ACS Database from a Dump File **E-10**

Compacting the CiscoSecure User Database **E-11**

User and AAA Client Import Option **E-13**

Importing User and AAA Client Information **E-13**

User and AAA Client Import File Format **E-15**

About User and AAA Client Import File Format **E-15**

ONLINE or OFFLINE Statement **E-16**

ADD Statements **E-16**

UPDATE Statements **E-18**

DELETE Statements **E-20**

ADD_NAS Statements **E-20**

DEL_NAS Statements **E-22**

Import File Examples **E-22**

Exporting User List to a Text File **E-23**

Exporting Group Information to a Text File **E-24**

Exporting Registry Information to a Text File **E-25**

Decoding Error Numbers **E-25**

Recalculating CRC Values **E-26**

Downloaded from www.Manualslib.com manuals search engine

User-Defined RADIUS Vendors and VSA Sets **E-27**
About User-Defined RADIUS Vendors and VSA Sets **E-27**
Adding a Custom RADIUS Vendor and VSA Set **E-28**
Deleting a Custom RADIUS Vendor and VSA Set **E-29**
Listing Custom RADIUS Vendors **E-30**
RADIUS Vendor/VSA Import File **E-31**
About the RADIUS Vendor/VSA Import File **E-32**
Vendor and VSA Set Definition **E-33**
Attribute Definition **E-34**
Enumeration Definition **E-35**
Example RADIUS Vendor/VSA Import File **E-37**

APPENDIX F **Cisco Secure ACS and Virtual Private Dial-up Networks F-1**
VPDN Process **F-1**

APPENDIX G **ODBC Import Definitions G-1**
accountActions Table Specification **G-1**
accountActions Table Format **G-2**
accountActions Table Mandatory Fields **G-3**
accountActions Table Processing Order **G-4**
Action Codes **G-5**
Action Codes for Setting and Deleting Values **G-5**
Action Codes for Creating and Modifying User Accounts **G-7**
Action Codes for Initializing and Modifying Access Filters **G-15**
Action Codes for Modifying TACACS+ and RADIUS Group and User Settings **G-20**
Action Codes for Modifying Network Configuration **G-27**

Downloaded from www.Manualslib.com manuals search engine

Action Code for Deleting the CiscoSecure User Database **G-31**

Cisco Secure ACS Attributes and Action Codes **G-31**

User-Specific Attributes **G-31**

User-Defined Attributes **G-34**

Group-Specific Attributes **G-34**

An Example accountActions Table **G-36**

APPENDIX H

Cisco Secure ACS Internal Architecture H-1

Windows NT/2000 Environment Overview **H-2**

Windows NT/2000 Services **H-2**

Windows NT/2000 Registry **H-2**

Cisco Secure ACS Web Server **H-2**

CSAdmin **H-3**

CSAuth **H-3**

CSDBSync **H-6**

CSLog **H-6**

CSMon **H-7**

Monitoring **H-7**

Recording **H-9**

Sample Scripts **H-10**

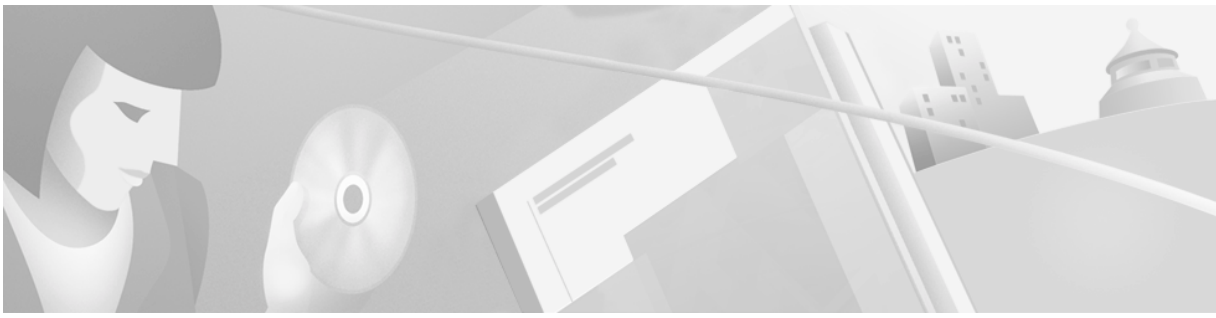
Configuration **H-10**

CSTacacs and CSRadius **H-11**

INDEX

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine



Preface

This section discusses the objectives, audience, and organization of the Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 User Guide.

Document Objectives

The objective of this document is to help you configure and use the Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) software and its features and utilities.

Who Should Read This Guide

This publication was written for system administrators who are using the Cisco Secure ACS software and are responsible for setting up and maintaining accounts and dial-in network security.

Downloaded from www.Manualslib.com manuals search engine

How This Guide is Organized

The Cisco Secure ACS User Guide is organized into the following chapters:

- Chapter 1, "Overview of Cisco Secure ACS." An overview of Cisco Secure ACS and its features, network diagrams, and system requirements.
- Chapter 2, "Deploying Cisco Secure ACS." A guide to deploying the Cisco Secure ACS that includes requirements, options, trade-offs, and suggested sequences.
- Chapter 3, "Setting Up the Cisco Secure ACS HTML Interface." Concepts and procedures regarding how to use the Interface Configuration section of the Cisco Secure ACS to configure the user interface.
- Chapter 4, "Setting Up and Managing Network Configuration." Concepts and procedures for Cisco Secure ACS network configuration and establishing a distributed system.
- Chapter 5, "Setting Up and Managing Shared Profile Components." Concepts and procedures regarding Cisco Secure ACS shared profile components: network access restrictions and device command sets.
- Chapter 6, "Setting Up and Managing User Groups." Concepts and procedures for establishing and maintaining Cisco Secure ACS user groups.
- Chapter 7, "Setting Up and Managing User Accounts". Concepts and procedures for establishing and maintaining Cisco Secure ACS user accounts.
- Chapter 8, "Establishing Cisco Secure ACS System Configuration." Concepts and procedures regarding the System Configuration portion of Cisco Secure ACS.
- Chapter 9, "Working with Logging and Reports." Concepts and procedures regarding Cisco Secure ACS logging and reports.
- Chapter 10, "Setting Up and Managing Administrators and Policy." Concepts and procedures for establishing and maintaining Cisco Secure ACS administrators.

Downloaded from www.Manualslib.com manuals search engine

- Chapter 11, “Working with User Databases.” Concepts and procedures for establishing user databases.
- Chapter 12, “Administering External User Databases.” Concepts and procedures for administering and maintaining user databases external to Cisco Secure ACS.

This guide also comprises the following appendixes:

- Appendix A, “Troubleshooting Information for Cisco Secure ACS.” How to identify and solve certain problems you might have with Cisco Secure ACS.
- Appendix B, “System Messages.” A list and explanation of most system messages you might encounter.
- Appendix C, “TACACS+ Attribute-Value Pairs.” A list of supported TACACS+ AV pairs and accounting AV pairs.
- Appendix D, “RADIUS Attributes.” A list of supported RADIUS AV pairs and accounting AV pairs.
- Appendix E, “Cisco Secure ACS Command-Line Database Utility.” Instructions for using the database import utility, CSUtil, to import an ODBC database, and back up, maintain, or restore the Cisco Secure ACS database.
- Appendix F, “Cisco Secure ACS and Virtual Private Dial-up Networks.” An introduction to Virtual Private Dial-up Networks (VPDN), including stripping and tunneling, with instructions for enabling VPDN on Cisco Secure ACS.
- Appendix G, “ODBC Import Definitions.” A list of ODBC import definitions, for use with the RDBMS Synchronization feature.
- Appendix H, “Cisco Secure ACS Internal Architecture.” A description of Cisco Secure ACS architectural components.

Downloaded from www.Manualslib.com manuals search engine

Conventions Used in This Guide

This guide uses the following typographical conventions:

Typographic Conventions	
Convention	**Meaning**
Italics	Introduces new or important terminology and variable input for commands.
`Script`	Denotes paths, file names, and example screen output. Also denotes Secure Script translations of security policy decision trees.
Bold	Identifies special terminology and options that should be selected during procedures.

Tip Means *the following information will help you solve a problem*. The tip's information might not be troubleshooting or even an action, but could be useful information.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a breach in your network security.

Warning **Means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translated versions of the warning, refer to the *Regulatory Compliance and Safety* document that accompanied the device.**

Downloaded from www.Manualslib.com manuals search engine

Related Documentation

Included in the Cisco Secure ACS HTML interface are two sources of information:

- Online Help contains information for each associated page in the Cisco Secure ACS HTML interface.
- Online Documentation is a complete copy of the *Cisco Secure ACS 3.0 for Windows 2000/NT Servers User Guide*.

We recommend that you read *Release Notes for Cisco Secure Access Control Server Version 3.0 for Windows 2000/NT Servers*. While a printed copy of this document comes with Cisco Secure ACS, check Cisco.com for the latest version.

You should also read the README.TXT file for additional important information.

Cisco Secure ACS includes an installation guide, *Installing Cisco Secure ACS 3.0 for Windows 2000/NT Servers*, to help you install the software efficiently and correctly.

Web Server Installation for Cisco Secure ACS for Windows 2000/NT User-Changeable Passwords contains information on installing and configuring the optional user-changeable password feature.

You can find other product literature, including white papers, data sheets, and product bulletins, at:

http://www.cisco.com/warp/public/cc/pd/sqsw/sq/prodlit/index.shtml.

You should refer to the documentation that came with your AAA clients for more information about those products. You might also want to consult the Cisco Systems publication *Cisco Systems' Internetworking Terms and Acronyms*.

Downloaded from www.Manualslib.com manuals search engine

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Downloaded from www.Manualslib.com manuals search engine

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Feedback** at the top of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

Downloaded from www.Manualslib.com manuals search engine

- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

Downloaded from www.Manualslib.com manuals search engine

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Overview of Cisco Secure ACS

This chapter provides an overview of Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS). It contains the following sections:

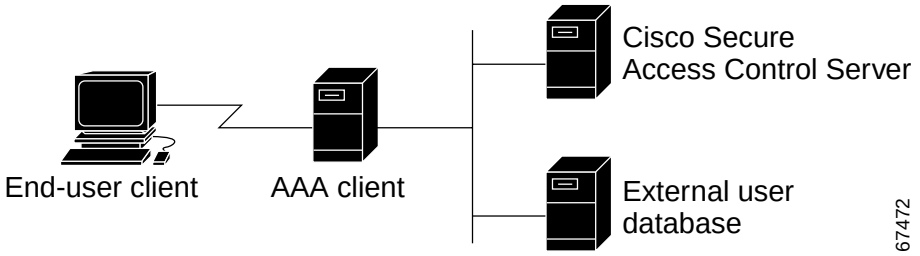
- The Cisco Secure ACS Paradigm, page 1-1
- Cisco Secure ACS Specifications, page 1-2
- AAA Server Functions and Concepts, page 1-4
- Cisco Secure ACS HTML Interface, page 1-21

The Cisco Secure ACS Paradigm

Cisco Secure ACS provides authentication, authorization, and accounting (AAA—pronounced “triple A”) services to network devices that function as AAA clients, such as a network access server, PIX Firewall, or router. The AAA client in Figure 1-1 on page 1-2 represents any such device that provides AAA client functionality and uses one of the AAA protocols supported by Cisco Secure ACS.

Downloaded from www.Manualslib.com manuals search engine

Figure 1-1 A Simple AAA Scenario



Cisco Secure ACS helps centralize access control and accounting, in addition to router and switch access management. With Cisco Secure ACS, network administrators can quickly administer accounts and globally change levels of service offerings for entire groups of users. Although the external user database shown in Figure 1-1 is optional, support for many popular user repository implementations enables companies to put to use the working knowledge gained from and the investment already made in building their corporate user repositories.

Cisco Secure ACS supports Cisco AAA clients such as the Cisco 2509, 2511, 3620, 3640, AS5200 and AS5300, AS5800, the Cisco PIX Firewall, Cisco Aironet Access Point wireless networking devices, Cisco VPN 3000 Concentrators, and Cisco VPN 5000 Concentrators. It also supports third-party devices that can be configured with the Terminal Access Controller Access Control System (TACACS+) or the Remote Access Dial-In User Service (RADIUS) protocol. Cisco Secure ACS treats all such devices as AAA clients. Cisco Secure ACS uses the TACACS+ and RADIUS protocols to provide AAA services that ensure a secure environment. For more information about support for TACACS+ and RADIUS in Cisco Secure ACS, see the "AAA Protocols—TACACS+ and RADIUS" section on page 1-5.

Cisco Secure ACS Specifications

This section provides information about Cisco Secure ACS performance specifications and the Windows services that compose Cisco Secure ACS.

Downloaded from www.Manualslib.com manuals search engine

System Performance Specifications

The performance capabilities of Cisco Secure ACS are largely dependent upon the Windows server it is installed upon, your network topology and network management, the selection of user databases, and other factors. For example, Cisco Secure ACS can perform many more authentications per second if it is running on a 1.4-GHz Pentium IV server with Windows 2000 Server on a 1 GB ethernet backbone than it can if it is running on a 200-MHz Pentium II server with Windows NT 4.0 on a 10 MB LAN.

For more information about the expected performance of Cisco Secure ACS in your network setting, contact your Cisco sales representative. The following items are general answers to common system performance questions. The performance of Cisco Secure ACS in your network depends on your specific environment and AAA requirements.

- **Maximum users supported by the CiscoSecure user database**—There is no theoretical limit to the number of users the CiscoSecure user database can support. We have successfully tested Cisco Secure ACS with databases in excess of 100,000 users. The practical limit for a single Cisco Secure ACS server authenticating against all its databases, internal and external, is approximately 300,000 to 500,000 users. This number increases significantly if the authentication load is spread across a number of replicated Cisco Secure ACS servers.
- **Transactions per second per number of users**—Assuming 10,000 users in the CiscoSecure user database, a single processor 300-MHz Pentium II server provides 80 RADIUS full login cycles (authentication, accounting start, and accounting stop) per second and approximately 40 TACACS+ logins per second. As the database grows, this performance declines roughly proportionately.
- **Maximum number of AAA clients supported**—Cisco Secure ACS can support AAA services for approximately 2000 network devices running a AAA client.

Cisco Secure ACS Windows Services

Cisco Secure ACS operates as a set of Windows NT or Windows 2000 services and controls the authentication, authorization, and accounting of users accessing networks.

Downloaded from www.Manualslib.com manuals search engine

When you install Cisco Secure ACS on your server, the installation adds several Windows services. The services provide the core of Cisco Secure ACS functionality. For a full discussion of each service, see the "Cisco Secure ACS Internal Architecture" section on page H-1. The Cisco Secure ACS services on your Cisco Secure ACS server include the following:

- **CSAdmin—**Provides the HTML interface for administration of Cisco Secure ACS.
- **CSAuth—**Provides authentication services.
- **CSDBSync—**Provides synchronization of the CiscoSecure user database with an external RDBMS application.
- **CSLog—**Provides logging services, both for accounting and system activity.
- **CSMon—**Provides monitoring, recording, and notification of Cisco Secure ACS performance, and includes automatic response to some scenarios.
- **CSTacacs—**Provides communication between TACACS+ AAA clients and the CSAuth service.
- **CSRadius—**Provides communication between RADIUS AAA clients and the CSAuth service.

Each module can be started and stopped individually from within the Microsoft Service Control Panel or as a group from within the Cisco Secure ACS HTML interface. For information about stopping and starting Cisco Secure ACS services, see the "Service Control" section on page 8-2.

AAA Server Functions and Concepts

Cisco Secure ACS is a AAA server, providing authentication, authorization, and accounting services to network devices that can act as AAA clients.

As a AAA server, Cisco Secure ACS incorporates many technologies to render AAA services to AAA clients. Understanding Cisco Secure ACS requires knowledge of many of these technologies. To address the most significant aspects, this section contains the following topics:

- Cisco Secure ACS and the AAA Client, page 1-5
- AAA Protocols—TACACS+ and RADIUS, page 1-5
- Authentication, page 1-7

Downloaded from www.Manualslib.com manuals search engine

- Authorization, page 1-15
- Accounting, page 1-17
- Administration, page 1-18

Cisco Secure ACS and the AAA Client

A AAA client is software running on a network device that enables the network device to defer authentication, authorization, and logging (accounting) of user sessions to a AAA server. AAA clients must be configured to direct all end-user client access requests to Cisco Secure ACS for authentication of users and authorization of service requests. Using the TACACS+ or RADIUS protocol, the AAA client sends authentication requests to Cisco Secure ACS.
Cisco Secure ACS verifies the username and password using the user databases it is configured to query. Cisco Secure ACS returns a success or failure response to the AAA client, which permits or denies user access, based on the response it receives. When the user authenticates successfully, Cisco Secure ACS sends a set of authorization attributes to the AAA client. The AAA client then begins forwarding accounting information to Cisco Secure ACS.

When the user has successfully authenticated, a set of session attributes can be sent to the AAA client to provide additional security and control of privileges, otherwise known as authorization. These attributes might include the IP address pool, access control list, or type of connection (for example, IP, IPX, or Telnet). More recently, networking vendors are expanding the use of the attribute sets returned to cover an increasingly wider aspect of user session provisioning.

AAA Protocols—TACACS+ and RADIUS

Cisco Secure ACS can use both the TACACS+ and RADIUS AAA protocols. Table 1-1 on page 1-6 provides a comparison of the two protocols.

Downloaded from www.Manualslib.com manuals search engine

Table 1-1 TACACS+ and RADIUS Protocol Comparison

TACACS+	RADIUS
TCP	**UDP**
Connection-oriented transport layer protocol, reliable full-duplex data transmission	Connectionless transport layer protocol, datagram exchange without acknowledgments or guaranteed delivery
Full packet encryption	Encrypts only passwords up to 16 bytes
Independent AAA architecture	Authentication and authorization combined
Useful for router management	Less intrinsically suited for router management

TACACS+

Cisco Secure ACS conforms to the TACACS+ protocol as defined by Cisco Systems in draft 1.77. For more information, refer to the Cisco IOS software documentation or Cisco.com (http://www.cisco.com).

RADIUS

Cisco Secure ACS conforms to the RADIUS protocol as defined in draft April 1997 and in the following Requests for Comments (RFCs):

- RFC 2138, Remote Authentication Dial In User Service
- RFC 2139, RADIUS Accounting
- RFC 2865
- RFC 2866
- RFC 2867
- RFC 2868

The ports used for authentication and accounting have changed in RADIUS RFC documents. To support both the older and newer RFCs, Cisco Secure ACS accepts authentication requests on port 1645 and port 1812. For accounting, Cisco Secure ACS accepts accounting packets on port 1646 and 1813.

Downloaded from www.Manualslib.com manuals search engine

In addition to support for standard IETF RADIUS attributes, Cisco Secure ACS includes support for RADIUS vendor-specific attributes (VSAs). We have predefined the following RADIUS VSAs in Cisco Secure ACS:

- Cisco IOS/PIX
- Cisco VPN 3000
- Cisco VPN 5000
- Ascend
- Juniper
- Microsoft
- Nortel

Cisco Secure ACS also supports up to 10 RADIUS VSAs that you define. After you define a new RADIUS VSA, you can use it as you would one of the RADIUS VSAs that come predefined in Cisco Secure ACS. In the Network Configuration section of the Cisco Secure ACS HTML interface, you can configure a AAA client to use a user-defined RADIUS VSA as its AAA protocol. In Interface Configuration, you can enable user-level and group-level attributes for user-defined RADIUS VSAs. In User Setup and Group Setup, you can configure the values for enabled attributes of a user-defined RADIUS VSA.

For more information about creating user-defined RADIUS VSAs, see the "User-Defined RADIUS Vendors and VSA Sets" section on page E-27.

Authentication

Authentication determines user identity and verifies the information. Traditional authentication uses a name and a fixed password. More modern and secure methods use technologies such as CHAP and one-time passwords (OTPs). Cisco Secure ACS supports a wide variety of these authentication methods.

There is a fundamental implicit relationship between authentication and authorization. The more authorization privileges granted to a user, the stronger the authentication should be. Cisco Secure ACS supports this fundamental relationship by providing various methods of authentication.

Downloaded from www.Manualslib.com manuals search engine

Authentication Considerations

Username and password is the most popular, simplest, and least expensive method used for authentication. No special equipment is required. This is a popular method for service providers because of its easy application by the client. The disadvantage is that this information can be told to someone else, guessed, or captured. Simple unencrypted username and password is not considered a strong authentication mechanism but can be sufficient for low authorization or privilege levels such as Internet access.

To reduce the risk of password capturing on the network, use encryption. Client and server access control protocols such as TACACS+ and RADIUS encrypt passwords to prevent them from being captured within a network. However, TACACS+ and RADIUS operate only between the AAA client and the access control server. Before this point in the authentication process, unauthorized persons can obtain clear-text passwords, such as the communication between an end-user client dialing up over a phone line or an ISDN line terminating at a network access server, or over a Telnet session between an end-user client and the hosting device.

Network administrators who offer increased levels of security services, and corporations that want to lessen the chance of intruder access resulting from password capturing, can use an OTP. Cisco Secure ACS supports several types of OTP solutions, including PAP for Point-to-Point Protocol (PPP) remote-node login. Token cards are considered one of the strongest OTP authentication mechanisms.

Authentication and User Databases

Cisco Secure ACS supports a variety of user databases. In addition to the CiscoSecure user database, Cisco Secure ACS supports several external user databases, including the following:

- Windows NT/2000 User Database
- Generic LDAP
- Novell NetWare Directory Services (NDS)
- Open Database Connectivity (ODBC)-compliant relational databases
- CRYPTOCard token server
- SafeWord token server

Downloaded from www.Manualslib.com manuals search engine

- AXENT token server
- RSA SecureID token server
- ActivCard token server
- Vasco token server

The various password protocols supported by Cisco Secure ACS for authentication are supported unevenly by the various databases supported by Cisco Secure ACS. Table 1-2 provides a reference of the password protocols supported by the various databases. For more information about the password protocols supported by Cisco Secure ACS, see the "Passwords" section on page 1-10.

Table 1-2 Password Authentication Protocol and User Database Compatibility

Database	ASCII	PAP	CHAP	ARAP	MS-CHAP v.1	MS-CHAP v.2	LEAP	EAP-CHAP	EAP-TLS
Cisco Secure ACS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	Yes	No	No	Yes	Yes	Yes	No	No
Windows AD	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes
Novell NDS	Yes	Yes	No	No	No	No	No	No	No
LDAP	Yes	Yes	No	No	No	No	No	No	Yes
ODBC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
LEAP Proxy RADIUS Server	No	No	No	No	Yes	No	Yes	No	No
ActivCard	Yes	Yes	No	No	No	No	No	No	No
CRYPTOCard	Yes	Yes	No	No	No	No	No	No	No
RADIUS Token Server	Yes	Yes	No	No	No	No	No	No	No
Vasco	Yes	Yes	No	No	No	No	No	No	No
AXENT	Yes	Yes	No	No	No	No	No	No	No
RSA	Yes	Yes	No	No	No	No	No	No	No
Safeword	Yes	Yes	No	No	No	No	No	No	No

Downloaded from www.Manualslib.com manuals search engine

Passwords

Cisco Secure ACS supports many common password protocols:

- ASCII/PAP
- CHAP
- MS-CHAP
- LEAP
- EAP-CHAP
- EAP-TLS
- ARAP

Passwords can be processed using these password authentication protocols based on the version and type of security control protocol used (for example, RADIUS or TACACS+) and the configuration of the AAA client and end-user client. The following sections outline the different conditions and functions of password handling.

In the case of token servers, Cisco Secure ACS acts as a client to the token server, either using its proprietary API or its RADIUS interface, depending on the token server. For more information, see the "About Token Servers and Cisco Secure ACS" section on page 11-48.

Different levels of security can be concurrently used with Cisco Secure ACS for different requirements. The basic user-to-network security level is PAP. Although it represents the unencrypted security, PAP does offer convenience and simplicity for the client. PAP allows authentication against the Windows NT/2000 database. With this configuration, users need to log in only once. CHAP allows a higher level of security for encrypting passwords when communicating from an end-user client to the AAA client. You can use CHAP with the CiscoSecure user database. ARAP support is included to support Apple clients.

Downloaded from www.Manualslib.com manuals search engine

Comparing PAP, CHAP, and ARAP

PAP, CHAP, and ARAP are authentication protocols used to encrypt passwords. However, each protocol provides a different level of security.

- **PAP—**Uses clear-text passwords (that is, unencrypted passwords) and is the least sophisticated authentication protocol. If you are using the Windows NT/2000 user database to authenticate users, you must use PAP password encryption or MS-CHAP.
- **CHAP—**Uses a challenge-response mechanism with one-way encryption on the response. CHAP enables Cisco Secure ACS to negotiate downward from the most secure to the least secure encryption mechanism, and it protects passwords transmitted in the process. CHAP passwords are reusable. If you are using the CiscoSecure user database for authentication, you can use either PAP or CHAP. CHAP does not work with the Windows NT/2000 user database.
- **ARAP—**Uses a two-way challenge-response mechanism. The AAA client challenges the end-user client to authenticate itself, and the end-user client challenges the AAA client to authenticate itself.

MS-CHAP

Cisco Secure ACS supports Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) for user authentication. Differences between MS-CHAP and standard CHAP are the following:

- The MS-CHAP Response packet is in a format compatible with Microsoft Windows NT/2000, Windows 95/98/ME, and LAN Manager 2.x. The MS-CHAP format does not require the authenticator to store a clear-text or reversibly encrypted password.
- MS-CHAP provides an authentication-retry mechanism controlled by the authenticator.
- MS-CHAP provides additional failure codes in the Failure packet Message field.

For more information on MS-CHAP, refer to RFC draft-ietf-pppext-mschap-00.txt, RADIUS Attributes for MS-CHAP Support.

Downloaded from www.Manualslib.com manuals search engine

Basic Password Configurations

There are several basic password configurations:

Note These configurations are all classed as inbound authentication.

- **Single password for ASCII/PAP/CHAP/MS-CHAP/ARAP—**This is the most convenient method for both the administrator when setting up accounts and the user when obtaining authentication. However, because the CHAP password is the same as the PAP password, and the PAP password is transmitted in clear text during an ASCII/PAP login, there is the chance that the CHAP password can be compromised.
- **Separate passwords for ASCII/PAP and CHAP/MS-CHAP/ARAP—**For a higher level of security, users can be given two separate passwords. If the ASCII/PAP password is compromised, the CHAP/ARAP password can remain secure.
- **External user database authentication—** For authentication by an external user database, the user does not need a password stored in the CiscoSecure user database. Instead, Cisco Secure ACS records which external user database it should query to authenticate the user.

Advanced Password Configurations

In addition to the basic password configurations listed above, Cisco Secure ACS supports the following:

- **Inbound passwords—** Passwords used by most Cisco Secure ACS users. These are supported by both the TACACS+ and RADIUS protocols. They are held internally to the CiscoSecure user database and are not usually given up to an external source if an outbound password has been configured.
- **Outbound passwords—**The TACACS+ protocol supports outbound passwords that can be used, for example, when a AAA client has to be authenticated by another AAA client and end-user client. Passwords from the CiscoSecure user database are then sent back to the second AAA client and end-user client.
- **Token caching—**When token caching is enabled, ISDN users can connect (for a limited time) a second B Channel using the same OTP entered during original authentication. For greater security, the B-Channel authentication

Downloaded from www.Manualslib.com manuals search engine

request from the AAA client should include the OTP in the username value (for example Fred*password*) while the password value contains an ASCII/PAP/ARAP password. The TACACS+ and RADIUS servers then verify that the token is still cached and validate the incoming password against either the single ASCII/PAP/ARAP or separate CHAP/ARAP password, depending on the user's configuration.

The TACACS+ SENDAUTH feature enables a AAA client to authenticate itself to another AAA client or an end-user client via outbound authentication. The outbound authentication can be PAP, CHAP, or ARAP. With outbound authentication, the Cisco Secure ACS password is given out. By default, the user's ASCII/PAP or CHAP/ARAP password is used, depending on how this has been configured; however, we recommend that the separate SENDAUTH password be configured for the user so that Cisco Secure ACS inbound passwords are never compromised.

If you want to use outbound passwords and maintain the highest level of security, we recommend that you configure users in the CiscoSecure user database with an outbound password that is different from the inbound password.

Password Aging

With Cisco Secure ACS you can choose whether and how you want to employ password aging. Control for password aging may reside either in the CiscoSecure user database, or in the Windows NT/2000 directory. Each password aging mechanism differs as to requirements and setting configurations.

The password aging feature controlled by the CiscoSecure user database enables you force users to change their passwords under any of the following conditions:

- After a specified number of days
- After a specified number of logins
- The first time a new user logs in

For information on the requirements and configuration of the password aging feature controlled by the CiscoSecure user database, see the "Enabling Password Aging for the CiscoSecure User Database" section on page 6-20.

The Windows NT/2000-based password aging feature enables you to control the following password aging parameters:

- Maximum password age in days
- Minimum password age in days

Downloaded from www.Manualslib.com manuals search engine

The methods and functionality of Windows password aging differ according to whether you are using Windows NT or Windows 2000 and whether you employ Active Directory (AD) or Security Accounts Manager (SAM). For information on the requirements and configuration of the Windows-based password aging feature, see the "Enabling Password Aging for Users in Windows Databases" section on page 6-25.

User-Changeable Passwords

With Cisco Secure ACS, you can install a separate program that enables users to change their passwords by using a web-based utility. For more information about installing user-changeable passwords, refer to the *Web Server Installation for Cisco Secure ACS for Windows NT/2000 User-Changeable Passwords* quick reference card.

Other Authentication-Related Features

In addition to the authentication-related features discussed in this section, the following features are provided by Cisco Secure ACS:

- Authentication of unknown users with external user databases (see the "Unknown User Processing" section on page 12-1)
- Microsoft Windows Callback feature (see the "Setting User Callback Option" section on page 7-10)
- Ability to import a UNIX password file to the CiscoSecure user database (see the "Importing User and AAA Client Information" section on page E-13)
- Ability for external users to authenticate via an enable password (see the "Setting TACACS+ Enable Password Options for a User" section on page 7-34)
- Proxy of authentication requests to other AAA servers (see the "Proxy in Distributed Systems" section on page 4-4)
- Configurable character string stripping from proxied authentication requests (see the "Stripping" section on page 4-6)

Downloaded from www.Manualslib.com manuals search engine

Authorization

Authorization determines what a user is allowed to do. Cisco Secure ACS can send user profile policies to a AAA client to determine the network services the user can access. You can configure authorization to give different users and groups different levels of service. For example, standard dial-up users might not have the same access privileges as premium customers and users. You can also differentiate by levels of security, access times, and services.

The Cisco Secure ACS access restrictions feature enables you to permit or deny logins based on time-of-day and day-of-week. For example, you could create a group for temporary accounts that can be disabled on specified dates. This would make it possible for a service provider to offer a 30-day free trial. The same authorization could be used to create a temporary account for a consultant with login permission limited to Monday through Friday, 9 A.M. to 5 P.M.

You can restrict users to a service or combination of services such as PPP, AppleTalk Remote Access (ARA), Serial Line Internet Protocol (SLIP), or EXEC. After a service is selected, you can restrict Layer 2 and Layer 3 protocols, such as IP and IPX, and you can apply individual access lists. Access lists on a per-user or per-group basis can restrict users from reaching parts of the network where critical information is stored or prevent them from using certain services such as File Transfer Protocol (FTP) or Simple Network Management Protocol (SNMP).

One fast-growing service being offered by service providers and adopted by corporations is a service authorization for Virtual Private Dial-Up Networks (VPDNs). Cisco Secure ACS can provide information to the network device for a specific user to configure a secure tunnel through a public network such as the Internet. The information can be for the access server (such as the home gateway for that user) or for the home gateway router to validate the user at the customer premises. In either case, Cisco Secure ACS can be used for each end of the VPDN.

Downloaded from www.Manualslib.com manuals search engine

Max Sessions

Max Sessions is a useful feature for organizations that need to limit the number of concurrent sessions available to either a user or a group:

- **User Max Sessions—**For example, an Internet service provider can limit each account holder to a single session.
- **Group Max Sessions—**For example, an enterprise administrator can allow the remote access infrastructure to be shared equally among several departments and limit the maximum number of concurrent sessions for all users in any one department.

In addition to simple User and Group Max Sessions control, Cisco Secure ACS enables the administrator to specify a Group Max Sessions value and a group-based User Max Sessions value; that is, a User Max Sessions value based on the user's group membership. For example, an administrator can allocate a Group Max Sessions value of 50 to the group "Sales" and also limit each member of the "Sales" group to 5 sessions each. This way no single member of a group account would be able to use more than 5 sessions at any one time, but the group could still have up to 50 active sessions.

Dynamic Usage Quotas

Cisco Secure ACS enables you to define usage quotas for users. You can limit the network access of each user in a group or of individual users. You define quotas by duration of sessions or the total number of sessions. Quotas can be either absolute or based on daily, weekly, or monthly periods. To grant access to users who have exceeded their quotas, you can reset session quota counters as needed.

To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated only when the user logs off and the accounting stop packet is received from the AAA client. If the AAA client through which the user is accessing your network fails, the session information is not updated. In the case of multiple sessions, such as with ISDN, the quota would not be updated until all sessions terminate, which means that a second channel will be accepted even if the first channel has exhausted the user's quota.

Downloaded from www.Manualslib.com manuals search engine

Other Authorization-Related Features

In addition to the authorization-related features discussed in this section, the following features are provided by Cisco Secure ACS:

- Group administration of users, with support for up to 500 groups (see the "Setting Up and Managing User Groups" section on page 6-1)
- Ability to map a user from an external user database to a specific Cisco Secure ACS group (see the "Database Group Mappings" section on page 12-10)
- Ability to disable an account after a number of failed attempts, specified by the administrator (see the "Setting Options for User Account Disablement" section on page 7-21)
- Ability to disable an account on a specific date (see the "Setting Options for User Account Disablement" section on page 7-21)
- Ability to restrict time-of-day and day-of-week access (see the "Setting Default Time of Day Access for a User Group" section on page 6-5)
- Ability to restrict network access based on remote address caller line identification (CLID) and dialed number identification service (DNIS) (see the "Setting Network Access Restrictions for a User Group" section on page 6-7)
- IP Pools for IP address assignment of end-user client hosts (see the "Setting IP Address Assignment Method for a User Group" section on page 6-26)
- Per-user and per-group TACACS+ or RADIUS attributes (see the "Advanced Options" section on page 3-4)
- Support for Voice over IP (VoIP), including configurable logging of accounting data (see the "Enabling VoIP Support for a User Group" section on page 6-4)

Accounting

AAA clients use the accounting functions provided by the RADIUS and TACACS+ protocols to communicate relevant data for each user session to the AAA server for recording. Cisco Secure ACS writes accounting records to a comma-separated value (CSV) log file or ODBC database, depending upon your

Downloaded from www.Manualslib.com manuals search engine

configuration. You can easily import these logs into popular database and spreadsheet applications for billing, security audits, and report generation. Among the types of accounting logs you can generate are the following:

- **TACACS+ Accounting—**Lists when sessions start and stop; records AAA client messages with username; provides caller line identification information; records the duration of each session.
- **RADIUS Accounting—**Lists when sessions stop and start; records AAA client messages with username; provides caller line identification information; records the duration of each session.
- **Administrative Accounting—**Lists commands entered on a network device with TACACS+ command authorization enabled.

For more information about Cisco Secure ACS logging capabilities, see Chapter 9, "Working with Logging and Reports".

Other Accounting-Related Features

In addition to the accounting-related features discussed in this section, the following features are provided by Cisco Secure ACS:

- Centralized logging, allowing several Cisco Secure ACS servers to forward their accounting data to a remote Cisco Secure ACS server (see the "Remote Logging" section on page 9-29)
- Configurable supplementary user ID fields for capturing additional information in logs (see the "User Data Configuration Options" section on page 3-3)
- Configurable logs, allowing you to capture as much information as needed (see the "Accounting Logs" section on page 9-4)

Administration

To configure, maintain, and protect its AAA functionality, Cisco Secure ACS provides a flexible administration scheme. You can perform nearly all administration of Cisco Secure ACS through its HTML interface.

Downloaded from www.Manualslib.com manuals search engine

You can access the HTML interface from computers other than the Cisco Secure ACS server. This enables remote administration of Cisco Secure ACS. For more information about the HTML interface, including steps for accessing the HTML interface, see the "Cisco Secure ACS HTML Interface" section on page 1-21.

HTTP Port Allocation for Remote Administrative Sessions

The HTTP port allocation feature allows you to configure the range of TCP ports used by Cisco Secure ACS for remote administrative HTTP sessions (that is, administrative sessions conducted by a browser running on a computer other than the Cisco Secure ACS server). Narrowing this range with the HTTP port allocation feature reduces the risk of unauthorized access to your network by a port open for administrative sessions.

We do not recommend that you administer Cisco Secure ACS through a firewall. Doing so requires that you configure the firewall to permit HTTP traffic over the range of HTTP administrative session ports that Cisco Secure ACS uses. While narrowing this range reduces the risk of unauthorized access, a greater risk of attack remains if you allow administration of Cisco Secure ACS from outside a firewall. A firewall configured to permit HTTP traffic over the Cisco Secure ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port a remote web browser must access to initiate an administrative session.

Note A broad HTTP port range could create a security risk. To prevent accidental discovery of an active administrative port by unauthorized users, keep the HTTP port range as narrow as possible. Cisco Secure ACS tracks the IP address associated with each remote administrative session. An unauthorized user would have to impersonate, or "spoof", the IP address of the legitimate remote host to make use of the active administrative session HTTP port.

For information about configuring the HTTP port allocation feature, see the "Access Policy" section on page 10-10.

Downloaded from www.Manualslib.com manuals search engine

Network Device Groups

With a network device group (NDG), you can view and administer a collection of AAA clients and AAA servers as a single logical group. To simplify administration, you can assign each group a convenient name that can be used to refer to all devices within that group. This creates two levels of network devices within Cisco Secure ACS—discrete devices such as an individual router, access server, AAA server, or PIX Firewall, and NDGs, which are named collection of AAA clients and AAA servers.

A network device can belong to only one NDG at a time.

Using NDGs enables an organization with a large number of AAA clients spread across a large geographical area to logically organize its environment within Cisco Secure ACS to reflect the physical setup. For example, all routers in Europe could belong to a group named Europe; all routers in the United States could belong to a US group; and so on. This would be especially convenient if each region's AAA clients were administered along the same divisions. Alternatively, the environment could be organized by some other attribute such as divisions, departments, business functions, and so on.

You can assign a group of users to an NDG. For more information on NDGs, see the "Network Device Group Configuration" section on page 4-20.

Other Administration-Related Features

In addition to the administration-related features discussed in this section, the following features are provided by Cisco Secure ACS:

- Ability to define different privileges per administrator (see the "Administrator Accounts" section on page 10-1)
- Ability to log administrator activities (see the "Administration Audit Log" section on page 9-17)
- Ability to view a list of logged-in users (see the "Logged-In Users Report" section on page 9-11)
- CSMonitor service, providing monitoring, notification, logging, and limited automated failure response (see the "Cisco Secure ACS Active Service Management" section on page 8-48)

Downloaded from www.Manualslib.com manuals search engine

- Ability to import of large numbers of users with the CSUtil.exe command-line utility (see the "Cisco Secure ACS Command-Line Database Utility" section on page E-1)
- Synchronization of the CiscoSecure user database with a relational database management system (RDBMS) (see the "RDBMS Synchronization" section on page 8-24)
- Replication of CiscoSecure user database components to other Cisco Secure ACS servers (see the "CiscoSecure Database Replication" section on page 8-6)
- Scheduled and on-demand Cisco Secure ACS system backups (see the "Cisco Secure ACS Backup" section on page 8-40)
- Ability to restore Cisco Secure ACS configuration, user accounts, and group profiles from a backup file (see the "Cisco Secure ACS System Restore" section on page 8-45)

Cisco Secure ACS HTML Interface

This section discusses the Cisco Secure ACS HTML interface and provides procedures for using it. This section contains the following topics:

- About the Cisco Secure ACS HTML Interface, page 1-21
- HTML Interface Layout, page 1-22
- Uniform Resource Locator for the HTML Interface, page 1-24
- Network Environments and Remote Administrative Sessions, page 1-24
- Accessing the HTML Interface, page 1-26
- Logging Off the HTML Interface, page 1-26
- Online Help and Online Documentation, page 1-27

About the Cisco Secure ACS HTML Interface

After installing Cisco Secure ACS, you configure and administer it through the HTML interface. The HTML interface enables you to easily modify Cisco Secure ACS configuration from any connection on your LAN or WAN.

Downloaded from www.Manualslib.com manuals search engine

The Cisco Secure ACS HTML interface is designed to be viewed using a web browser. The design primarily uses HTML, along with some Java functions, to enhance ease of use. This design keeps the interface responsive and straightforward. The inclusion of Java requires that the browser used for administrative sessions supports Java. For a list of supported browsers, see the Release Notes. The latest revision to the Release Notes is posted on Cisco.com (http://www.cisco.com).

The HTML interface not only makes viewing and editing user and group information possible, it also enables you to restart services, add remote administrators, change AAA client information, back up the system, view reports from anywhere on the network, and more. The reports track connection activity, show which users are logged in, list the failed authentication and authorization attempts, and show administrators' recent tasks.

HTML Interface Layout

The HTML interface has three vertical partitions, known as frames:

- **Navigation Bar—**The gray frame on the left of the browser window, the navigation bar contains the task buttons. Each button changes the configuration area (see below) to a unique section of the Cisco Secure ACS application, such as the User Setup section or the Interface Configuration section. This frame does not change; it always contains the following buttons:
  - **User Setup—**Add and edit user profiles
  - **Group Setup—**Configure network services and protocols for groups of users
  - **Shared Profile Components—**Add and edit network access restriction and command authorization sets, to be applied to users and groups
  - **Network Configuration—**Add and edit network access devices and configure distributed systems
  - **System Configuration—**Configure database information and accounting
  - **Interface Configuration—**Display or hide product features and options to be configured
  - **Administration Control—**Define and configure access policies

Downloaded from www.Manualslib.com manuals search engine

  - **External User Databases—**Configure external databases for authentication
  - **Reports and Activity—**Display accounting and logging information
  - **Online Documentation—**View the *Cisco Secure ACS User Guide*

- **Configuration Area—**The frame in the middle of the browser window, the configuration area displays web pages that belong to one of the sections represented by the buttons in the navigation bar. The configuration area is where you add, edit, or delete information. For example, you configure user information in this frame on the User Setup Edit page.

Note Most pages have a Submit button at the bottom. Click Submit to confirm your changes. If you do not click Submit, changes are not saved.

- **Display Area—**The frame on the right of the browser window, the display area shows one of the following options:
  - **Online Help—**Displays basic help about the page currently shown in the configuration area. This help is not intended to offer in-depth information, but rather give some basic information about what can be accomplished in the middle frame. For more detailed information, click Section Information at the bottom of the page to go to the applicable part of Online Documentation.
  - **Reports or Lists—**Displays lists or reports, including accounting reports. For example, in User Setup you can show all usernames that start with a specific letter. The list of usernames beginning with a specified letter is displayed in this section. The usernames are hyperlinks to the specific user configuration, so clicking the name enables you to edit that user.
  - **System Messages—**Displays messages after you click Submit if you have typed in incorrect or incomplete data. For example, if the information you entered in the Password box does not match the information in the Confirm Password box in the User Setup section, Cisco Secure ACS displays an error message here. The incorrect information remains in the configuration area so that you can retype and resubmit the information correctly.

Downloaded from www.Manualslib.com manuals search engine

Uniform Resource Locator for the HTML Interface

The HTML interface is available by web browser at one of the following uniform resource locators (URLs):

- http://*Windows server IP address*:2002
- http://*Windows server host name*:2002

From the server on which Cisco Secure ACS is installed, you can also use the following URLs:

- http://*localhost*:2002
- http://127.0.0.1:2002

Network Environments and Remote Administrative Sessions

We recommend that remote administrative sessions take place without the use of an HTTP proxy server, without a firewall between the remote browser and the Cisco Secure ACS server, and without a NAT gateway between the remote browser and the Cisco Secure ACS server. Because these limitations are not always practical, we included the following topics regarding these remote administration scenarios.

Remote Administrative Sessions and HTTP Proxy

Cisco Secure ACS does not support HTTP proxy for remote administrative sessions. If the browser used for a remote administrative session is configured to use a proxy server, Cisco Secure ACS sees the administrative session originating from the IP address of the proxy server rather than the actual address of the remote workstation. Remote administrative session tracking assumes each browser resides on a workstation with a unique IP.

Also, IP filtering of proxied administrative sessions has to be based on the IP address of the proxy server rather than the IP address of the workstation. This conflicts with administrative session communication that does use the actual IP address of the workstation. For more information about IP filtering of remote administrative sessions, see the "Access Policy" section on page 10-10.

Downloaded from www.Manualslib.com manuals search engine

For these reasons, we do not recommend performing administrative sessions using a web browser that is configured to use a proxy server. Administrative sessions using a proxy-enabled web browser is not tested. If your web browser is configured to use a proxy server, disable HTTP proxying when attempting remote Cisco Secure ACS administrative sessions.

Remote Administrative Sessions through Firewalls

In the case of firewalls that do no perform network address translation (NAT), remote administrative sessions conducted across the firewall can require additional configuration of Cisco Secure ACS and the firewall. This is because Cisco Secure ACS assigns a random HTTP port at the beginning of a remote administrative session.

To allow remote administrative sessions from browsers outside a firewall that protects a Cisco Secure ACS server, the firewall must allow HTTP traffic across the range of ports that Cisco Secure ACS is configured to use. You can control the HTTP port range using the HTTP port allocation feature. For more information about the HTTP port allocation feature, see the "HTTP Port Allocation for Remote Administrative Sessions" section on page 1-19.

While administering Cisco Secure ACS through a firewall that is not performing NAT is possible, we do not recommend that you administer Cisco Secure ACS through a firewall. For more information, see the "HTTP Port Allocation for Remote Administrative Sessions" section on page 1-19.

Remote Administrative Sessions through a NAT Gateway

We do not recommend conducting remote administrative sessions across a network device performing NAT. If the administrator runs a browser on a workstation behind a NAT gateway, Cisco Secure ACS receives the HTTP requests from the NAT device's public IP address, which conflicts with the workstation's private IP address, included in the content of the HTTP requests. Cisco Secure ACS does not permit this.

If the Cisco Secure ACS server is behind a NAT gateway, you could configure the gateway to forward all connections to port 2002 to the Cisco Secure ACS server, using the same port. Additionally, all the ports allowed using the HTTP port allocation feature would have to be similarly mapped. We have not tested such a configuration and do not recommend implementing it.

Downloaded from www.Manualslib.com manuals search engine

Accessing the HTML Interface

Remote administrative sessions always require that you login using a valid administrator name and password, as configured in the Administration Control section. If the Allow automatic local login check box is cleared on the Sessions Policy Setup page in the Administration Control section, Cisco Secure ACS requires a valid administrator name and password for administrative sessions accessed from a browser on the Cisco Secure ACS server.

To access the HTML interface, follow these steps:

Step 1 Open a web browser. For a list of supported web browsers, see the Release Notes for the version of Cisco Secure ACS you are accessing. The latest revision to the Release Notes is posted on Cisco.com (http://www.cisco.com).

Step 2 In the Address or Location bar in the web browser, type the applicable URL. For a list of possible URLs, see the "Uniform Resource Locator for the HTML Interface" section on page 1-24.

Step 3 If the Cisco Secure ACS for Windows 2000/NT Login page appears, follow these steps:

a. In the **Username** box, type a valid Cisco Secure ACS administrator name.

b. In the **Password** box, type the password for the administrator name you specified.

c. Click **Login**.

Result: The Cisco Secure ACS for Windows 2000/NT initial page appears.

Logging Off the HTML Interface

When you are finished using the HTML interface, we recommend that you log off. While Cisco Secure ACS can timeout unused administrative sessions, logging off prevents unauthorized access by someone using the browser after you or by unauthorized persons using the HTTP port left open to support the administrative session.

To log off the Cisco Secure ACS HTML interface, click the **Logoff** button.

Downloaded from www.Manualslib.com manuals search engine

Note The Logoff button appears in the upper right corner of the browser window, except on the initial page, where it appears in the upper left of the configuration area.

Online Help and Online Documentation

We provide two sources of information in the HTML interface:

- **Online Help**—Contains basic information about the page shown in the configuration area.
- **Online Documentation**—Contains the entire user guide.

Using Online Help

Online help is the default content in the display area. For every page that appears in the configuration area, there is a corresponding online help page. At the top of each online help page is a list of topics covered by that page.

To jump from the top of the online help page to a particular topic, click the topic name in the list at the top of the page.

There are three icons that appear on many pages in Cisco Secure ACS:

- **Question Mark**—Many subsections of the pages in the configuration area contain an icon with a question mark. To jump to the applicable topic in an online help page, click the question mark icon.
- **Section Information**—Many online help pages contain a Section Information icon at the bottom of the page. To view an applicable section of the online documentation, click the Section Information icon.
- **Back to Help**—Wherever you find a online help page with a Section Information icon, the corresponding page in the configuration area contains a Back to Help icon. If you have accessed the online documentation by clicking a Section Information icon and want to view the online help page again, click the Back to Help icon.

Downloaded from www.Manualslib.com manuals search engine

Using the Online Documentation

The Cisco Secure ACS online documentation is the user guide for Cisco Secure ACS. The user guide provides information about the configuration, operation, and concepts of Cisco Secure ACS. The information presented in the online documentation is as current as the release date of the Cisco Secure ACS version you are using. For the most up-to-date documentation about Cisco Secure ACS, please go to http://www.cisco.com

Tip Click **Section Information** on any online help page to view online documentation relevant to the section of the HTML interface you are using.

To access online documentation, follow these steps:

Step 1 In the Cisco Secure ACS HTML interface, click **Online Documentation**.

Tip To open the online documentation in a new browser window, right-click **Online Documentation**, and then click **Open Link in New Window** (for Microsoft Internet Explorer) or **Open in New Window** (for Netscape Navigator).

Result: The table of contents opens in the configuration area.

Step 2 To select a topic from the table of contents, scroll through the table of contents and click the applicable topic.

Result: The online documentation for the topic selected appears in the display area.

Step 3 To select a topic from the index, follow these steps:

a. Click **[Index]**.

Result: The index appears in the display area.

b. Scroll through the index to find an entry for the topic you are researching.

Tip Use the lettered shortcut links to jump to a particular section of the index.

Downloaded from www.Manualslib.com manuals search engine

Result: Entries appear with numbered links after them. The numbered links lead to separate instances of the entry topic.

c. Click an instance number for the desired topic.

Result: The online documentation for the topic selected appears in the display area.

Step 4 To print the online documentation, click in the display area, and then click **Print** in your browser's navigation bar.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Deploying Cisco Secure ACS

Deployment of Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) can be a complex and iterative process that differs depending on the specific implementation required. This chapter provides insight into many aspects of the deployment process; it is designed not as a one-size-fits-all procedure, but as a collection of interconnected factors that you should consider before you install Cisco Secure ACS.

The level of complexity in deploying Cisco Secure ACS reflects the evolving nature of AAA servers in general, and the advanced capabilities, flexibility, and features of Cisco Secure ACS in particular. When AAA was first conceived, its main purpose was to provide a centralized point of control for user access via dial-up services. As user databases grew and the locations of the access servers became more dispersed, more capability was required of the AAA server. Regional, then global, requirements became common. Today, Cisco Secure ACS is required to provide AAA services for dial-up access, dial-out access, wireless, VLAN access, firewalls, VPN concentrators, administrative controls, and more. The list of external databases supported has also continued to grow and the employment of multiple databases, as well as multiple Cisco Secure ACSs, has become more common. Regardless of the scope of your particular Cisco Secure ACS deployment, the information contained in this chapter should prove valuable. If you have particular deployment questions not addressed in this guide, contact your Cisco technical representative for assistance.

This chapter contains the following sections:

- Basic Deployment Requirements for Cisco Secure ACS, page 2-2
- Basic Deployment Factors for Cisco Secure ACS, page 2-4
- Suggested Deployment Sequence, page 2-18

Downloaded from www.Manualslib.com manuals search engine

Basic Deployment Requirements for Cisco Secure ACS

This section details the minimum requirements you must meet to be able to successfully deploy Cisco Secure ACS. The following topics are covered:

- System Requirements, page 2-2
  - Hardware Requirements, page 2-2
  - Operating System Requirements, page 2-3
  - Third-Party Software Requirements, page 2-3
- Network Requirements, page 2-4

System Requirements

Your Cisco Secure ACS server must meet the minimum hardware and software requirements detailed in the sections that follow.

Hardware Requirements

Your Cisco Secure ACS server must meet the following minimum hardware requirements:

- Pentium III processor, 550 MHz or faster
- 256 MB of RAM
- At least 250 MB of free disk space. If you are running your database on the same machine, more disk space is required.
- Minimum graphics resolution of 256 colors at 800 x 600 lines

Downloaded from www.Manualslib.com manuals search engine

Operating System Requirements

Your Cisco Secure ACS server must have an English-language version of one of the following Microsoft Windows operating systems installed:

- Windows 2000 Server with Service Pack 1 or Service Pack 2 installed
- Windows 2000 Advanced Server, with these additional requirements:
  - without Microsoft Clustering Services installed
  - with Service Pack 1 or Service Pack 2 installed.
- Windows 2000 Datacenter Server, with these additional requirements:
  - without Microsoft Clustering Services installed
  - with Service Pack 1 or Service Pack 2 installed.
- Windows NT Server 4.0 with Service Pack 6a installed.

Windows Service Packs can be applied either before or after installing Cisco Secure ACS. If you do not install a required Service Pack before installing Cisco Secure ACS, the Cisco Secure ACS installation program warns you that the required Service Pack is not present on your server. If you receive a Service Pack message, continue the installation, and then install the required Service Pack before starting user authentication with Cisco Secure ACS.

For the latest information about tested operating systems and service packs, see the Release Notes. The latest version of the Release Notes are posted at http://www.cisco.com.

Third-Party Software Requirements

Your Cisco Secure ACS server must have a compatible browser installed. Cisco Secure ACS has been tested with the following browsers on Microsoft Windows operating systems:

- Microsoft Internet Explorer 5.0 and 5.5
- Netscape Communicator 4.76

Note Both Java and JavaScript must be enabled in browsers used to administer Cisco Secure ACS.

Downloaded from www.Manualslib.com manuals search engine

For the latest information about tested browsers and other third-party applications, such as Novell NDS clients and token-card clients, see the Release Notes. The latest version of the Release Notes is posted on http://www.cisco.com.

Network Requirements

Your network should meet the following requirements before you begin installing Cisco Secure ACS.

- To have Cisco Secure ACS use the Grant Dial-in Permission to User feature in Windows when authorizing network users, make sure this option is checked in the Windows NT User Manager or Windows 2000 Active Directory Users and Computers for the applicable user accounts.
- For full TACACS+ and RADIUS support on Cisco IOS devices, make sure that your AAA clients are running Cisco IOS Release 11.2 or later.
- Make sure that any non-Cisco IOS AAA clients can be configured with TACACS+ and/or RADIUS.
- Make sure that dial-in, VPN, or wireless clients can successfully connect to the applicable AAA clients.
- Make sure that the Windows server can ping AAA clients.
- Make sure a compatible web browser is installed on the Windows server. For more information, see the "Third-Party Software Requirements" section on page 2-3.

Basic Deployment Factors for Cisco Secure ACS

Generally, the ease in deploying Cisco Secure ACS is directly related to the complexity of the implementation planned and the degree to which you have defined your policies and requirements. This section presents some of the basic factors you should consider before you begin implementing Cisco Secure ACS.

This section includes the following topics:

- Network Topology, page 2-5
- Remote Access Policy, page 2-13
- Security Policy, page 2-14

Downloaded from www.Manualslib.com manuals search engine

- Administrative Access Policy, page 2-14
- Database, page 2-17
- Network Speed and Reliability, page 2-18

Network Topology

How the enterprise network is configured is likely to be the single most important factor in deciding how to deploy Cisco Secure ACS. While an exhaustive treatment of this topic is beyond the scope of this guide, this section details how the growth of network topology options has made Cisco Secure ACS deployment decisions more complex.

When AAA was first considered, network access was restricted to either devices directly connected to the LAN or remote devices gaining access via modem. Today, enterprise networks can be very complex and, thanks to tunneling technologies, can be widely geographically dispersed.

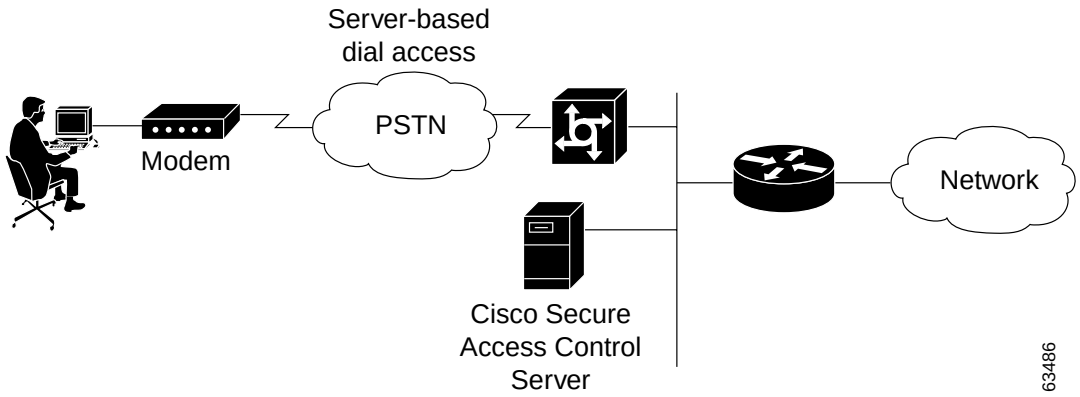
Dial-Up Topology

In the traditional model of dial-up access (a PPP connection), a user employing a modem or ISDN connection is granted access to an intranet via a network access server (NAS) functioning as a AAA client. Users may be able to connect via only a single AAA client as in a small business, or have the option of numerous geographically dispersed AAA clients.

In the small LAN environment, see Figure 2-1 on page 2-6, network architects typically place a single Cisco Secure ACS internal to the AAA client, protected from outside access by means of a firewall and the AAA client. In this environment, the user database is usually small, there are few devices that require access to the Cisco Secure ACS for AAA, and any database replication is limited to a secondary Cisco Secure ACS as a backup.

Downloaded from www.Manualslib.com manuals search engine

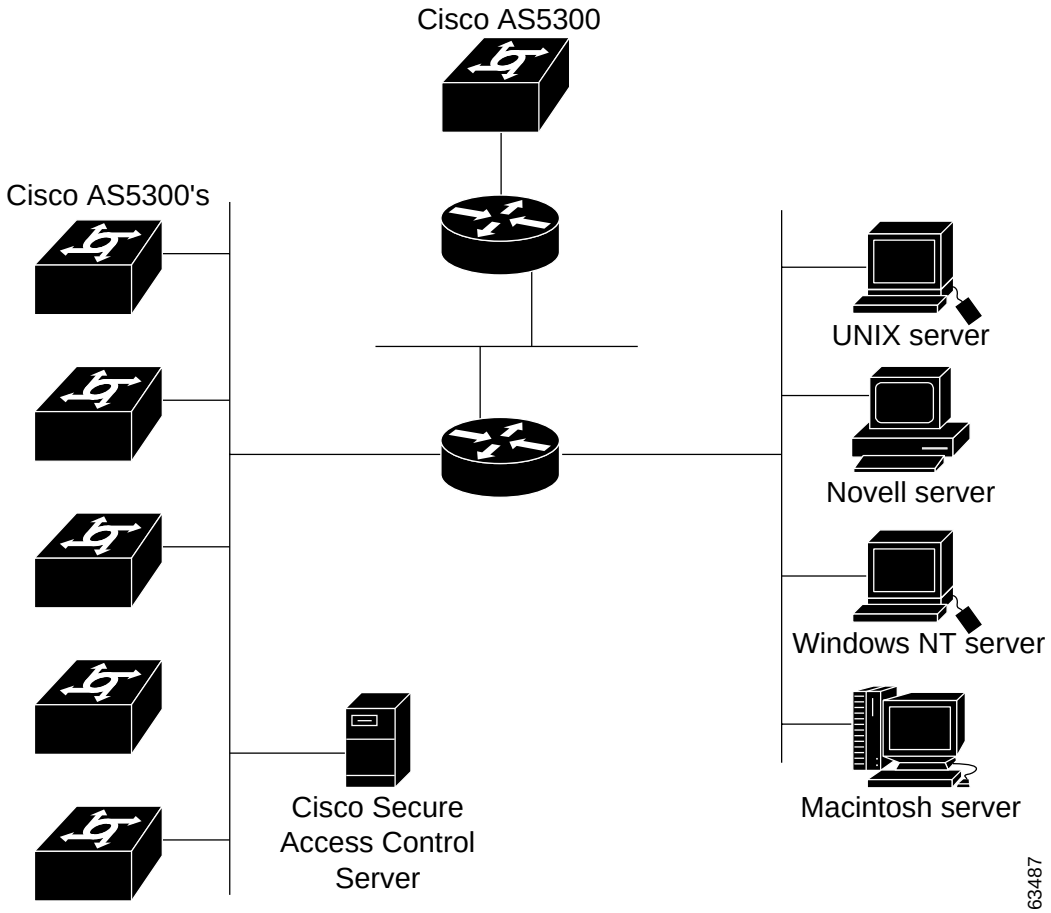
Figure 2-1 Small Dial-up Network



In a larger dial-in environment, a single Cisco Secure ACS installation with a backup may be suitable, too. The suitability of this configuration is dependent on network and server access latency. Figure 2-2 on page 2-7 shows an example of a large dial-in arrangement. In this scenario the addition of a backup Cisco Secure ACS unit is a recommended addition.

Downloaded from www.Manualslib.com manuals search engine

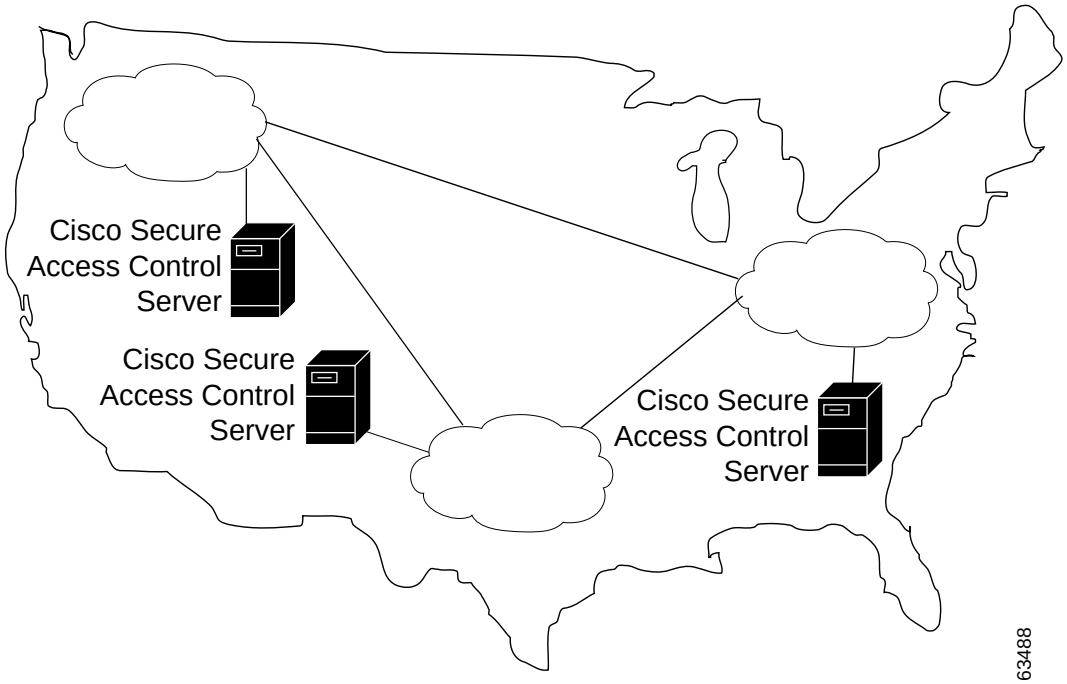
Figure 2-2 Large Dial-up Network



In a very large, geographically dispersed network, see Figure 2-3 on page 2-8, there may be access servers located in different parts of a city, in different cities, or in different continents. A central Cisco Secure ACS may work if network latency is not an issue, but connection reliability over long distances may cause problems. In this case, local Cisco Secure ACS installations may be preferable to a central server. If the need for a globally coherent user database is paramount, database replication or synchronization from a central server may be necessary. This may be further complicated by the use of external databases (such as Windows NT/2000 or the Lightweight Directory Access Protocol [LDAP]) for authentication. Additional security measures may be required to protect the network and user information being forwarded across the WAN. This combines topology and security factors. Such a case calls for adding an encrypted connection between regions.

Downloaded from www.Manualslib.com manuals search engine

Figure 2-3 Geographically Dispersed Network



Wireless Network

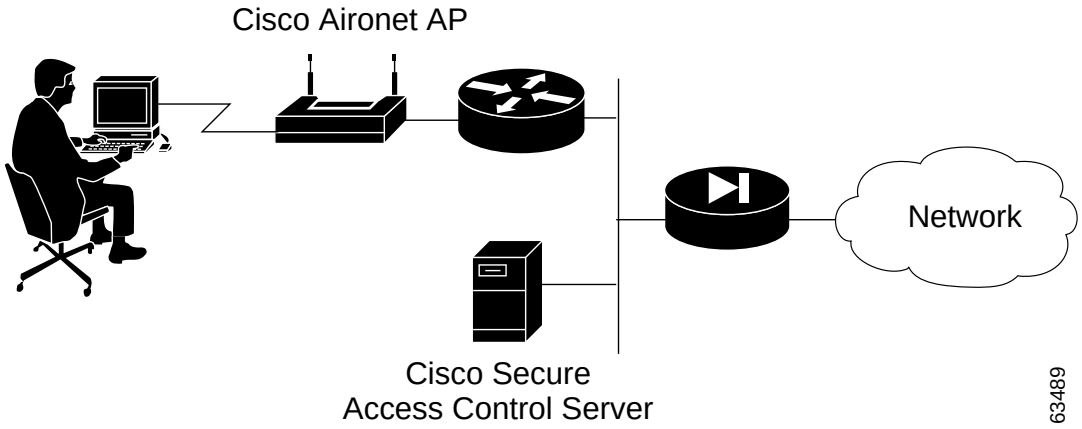
The wireless network access point is a relatively new client for AAA services. The wireless access point (AP), such as the Cisco Aironet series, provides a bridged connection for mobile end-user clients into the LAN. Authentication is absolutely necessary due to the ease of access to the AP. Encryption is also a necessity because of the ease of eavesdropping on communications. As such, security plays an even bigger role than in the dial-up scenario and is discussed in more detail later in this section.

Scaling can be a serious issue in the wireless network. Like the “wired” LAN, the mobility factor of the wireless LAN (WLAN) requires considerations similar to those given to the dial-up network. Unlike the wired LAN, however, the WLAN can be more readily expanded. Though WLAN technology does have physical limits as to the number of users that can be connected via an AP, the number of APs can grow quickly. As with the dial-up network, you can structure your WLAN to allow full access for all users, or to provide restricted access to different subnets between sites, buildings, floors, or rooms. This brings up a unique issue with the WLAN: the ability of a user to “roam” between APs.

Downloaded from www.Manualslib.com manuals search engine

In the simple WLAN, there may be a single AP installed; see Figure 2-4. Because there is only one AP, the primary issue is security. In this environment, there is generally a small user base and few network devices to worry about. Providing AAA services to the other devices on the network does not cause any significant additional load on the Cisco Secure ACS.

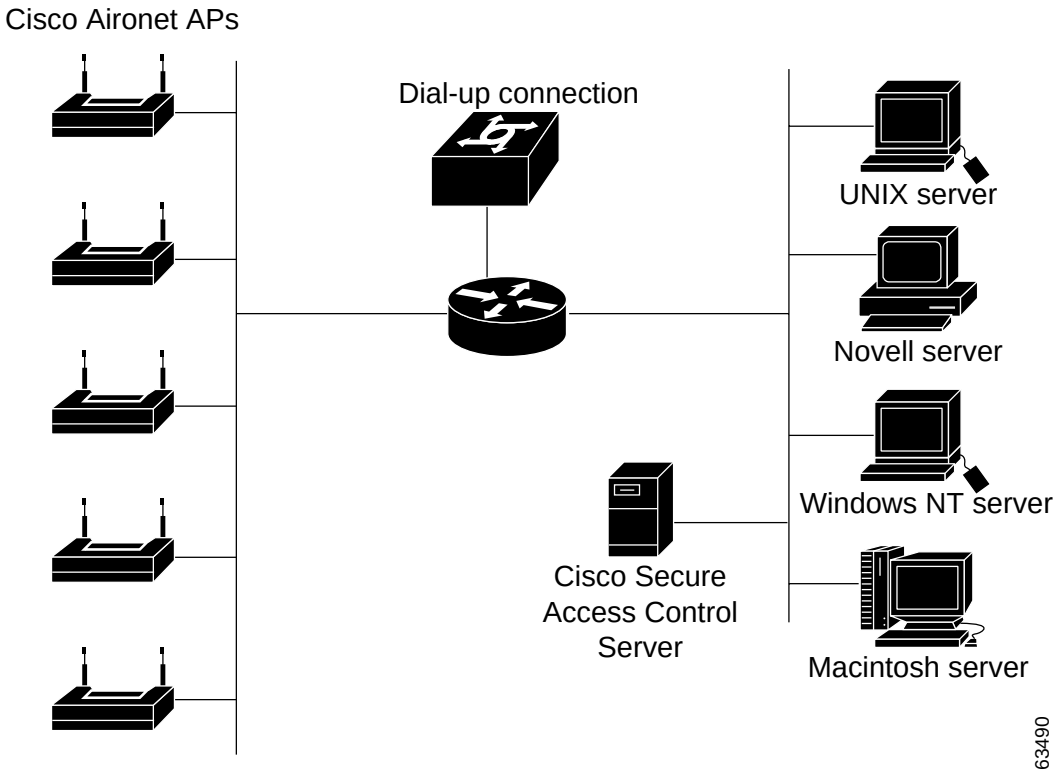
Figure 2-4 Simple WLAN



In the LAN where a number of APs are deployed, as in a large building or a campus environment, your decisions on how to deploy Cisco Secure ACS become a little more involved. Though Figure 2-5 on page 2-10 shows all APs on the same LAN, they may be distributed throughout the LAN, connected via routers, switches, and so forth. In the larger, geographical distribution of WLANs, deployment of Cisco Secure ACS is similar to that of large regional distribution of dial-up LANs; see Figure 2-3 on page 2-8.

Downloaded from www.Manualslib.com manuals search engine

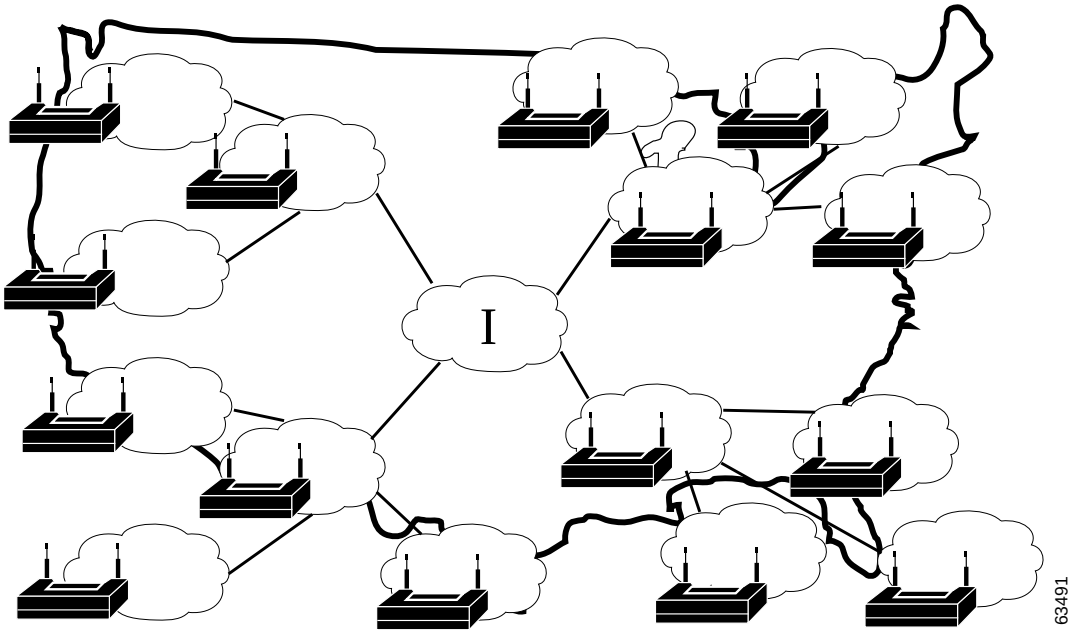
Figure 2-5 Campus WLAN



This is particularly true when the regional topology is the campus WLAN. This model starts to change when you deploy WLANs in many small sites that more resemble the simple WLAN shown in Figure 2-4 on page 2-9. This model may be applicable to a chain of small stores distributed throughout a city or state, nationally, or globally; see Figure 2-6 on page 2-11.

Downloaded from www.Manualslib.com manuals search engine

Figure 2-6 Large Deployment of Small Sites



For the model in Figure 2-6, the decision where to site Cisco Secure ACS depends on whether users from the entire network need access on any AP, or whether they only require regional or local network access. This, along with database type, controls whether local or regional Cisco Secure ACS installations are required, and how database continuity is maintained. In this very large deployment model, security becomes a more complicated issue, too.

Remote Access using VPN

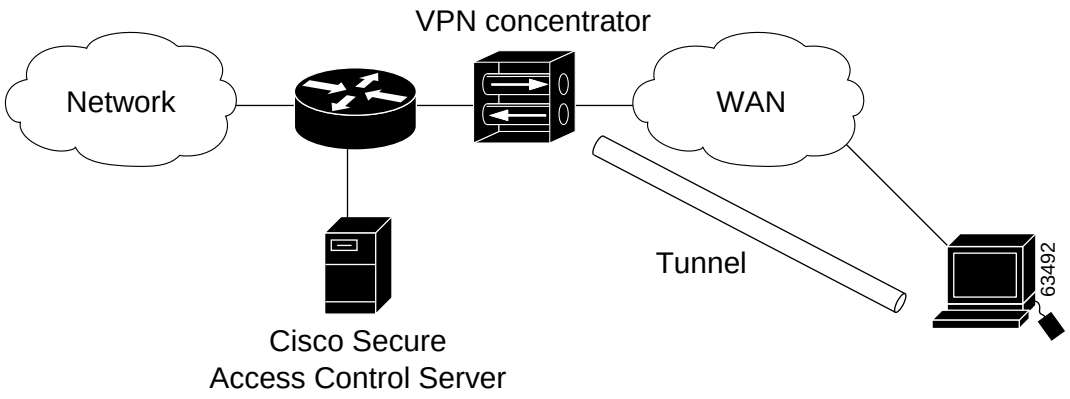
Virtual Private Networks (VPNs) use advanced encryption and tunneling to permit organizations to establish secure, end-to-end, private network connections over third-party networks, such as the Internet or extranets; see Figure 2-7 on page 2-12. The benefits of a VPN include the following:

- **Cost Savings**—By leveraging third-party networks with VPN, organizations no longer have to use expensive leased or frame relay lines and can connect remote users to their corporate networks via a local Internet service provider (ISP) instead of via expensive 800-number or long distance calls to resource-consuming modem banks.

Downloaded from www.Manualslib.com manuals search engine

- **Security**—VPNs provide the highest level of security using advanced encryption and authentication protocols that protect data from unauthorized access.
- **Scalability**—VPNs allow corporations to use remote access infrastructure within ISPs. Therefore, corporations can add a virtually unlimited amount of capacity without adding significant infrastructure.
- **Compatibility with Broadband Technology**—VPNs allow mobile workers, telecommuters, and day extenders to take advantage of high-speed, broadband connectivity, such as DSL and cable, when gaining access to their corporate networks, providing workers significant flexibility and efficiency.

Figure 2-7 Simple VPN Configuration



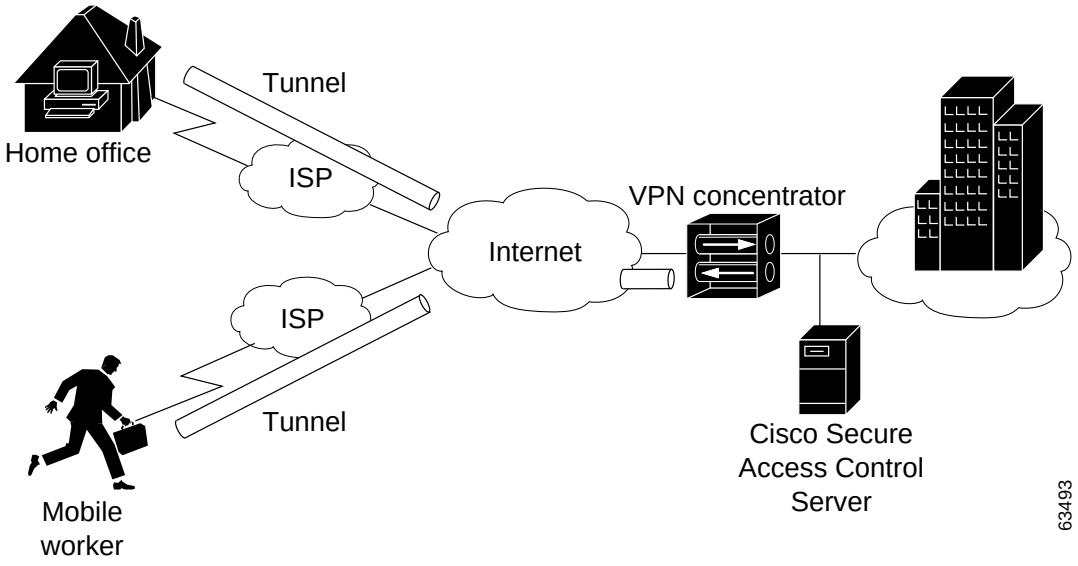
There are two types of VPN access into a network, as follows:

- **Site-to-Site VPNs**—Extend the classic WAN by providing large-scale encryption between multiple fixed sites such as remote offices and central offices, over a public network, such as the Internet.
- **Remote Access VPNs**—Permit secure, encrypted connections between mobile or remote users and their corporate networks via a third-party network, such as a service provider, via VPN client software.

Generally speaking, site-to-site VPNs can be viewed as a typical WAN connection and are not usually configured to use AAA to secure the initial connection and are likely to use the device-oriented IPSec tunneling protocol. Remote Access VPNs, however, are similar to classic remote connection technology (modem/ISDN) and lend themselves to using the AAA model very effectively; see Figure 2-8 on page 2-13.

Downloaded from www.Manualslib.com manuals search engine

Figure 2-8 Enterprise VPN Solution



For more information about implementing VPN solutions, see the reference guide *A Primer for Implementing a Cisco Virtual Private Network.*

Remote Access Policy

Remote access is a broad concept. In general, it defines how the user can connect to the LAN, or from the LAN to outside resources (that is, the Internet). There are several ways this may occur. The methods include dial-in, ISDN, wireless bridges, and secure internet connections. Each method incurs its own advantages and disadvantages, and provides a unique challenge to providing AAA services. This closely ties remote access policy to the enterprise network topology. In addition to the method of access, other decisions can also affect how Cisco Secure ACS is deployed; these include: specific network routing (access lists), time-of-day access, individual restrictions on AAA client access, access control lists (ACLs), and so on.

Remote access policies can be implemented for employees who telecommute or for mobile users who dial in over ISDN or public switched telephone network (PSTN). Such policies are enforced at the corporate campus with Cisco Secure ACS and the AAA client. Inside the enterprise network, remote access policies can control wireless access by individual employees.

Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS remote access policy provides control by using central authentication and authorization of remote users. The CiscoSecure user database maintains all user IDs, passwords, and privileges. Cisco Secure ACS access policies can be downloaded in the form of ACLs to network access servers such as the Cisco AS5300 Network Access Server, or by allowing access during specific periods, or on specific access servers.

The remote access policy is part of the overall corporate security policy.

Security Policy

We recommend that every organization that maintains a network develop a security policy for the organization. The sophistication, nature, and scope of your security policy directly affect how you deploy Cisco Secure ACS.

For more information about developing and maintaining a comprehensive security policy, refer to the following documents:

- *Network Security Policy: Best Practices White Paper*
- *Delivering End-to-End Security in Policy-Based Networks*
- *Cisco IOS Security Configuration Guide*

Administrative Access Policy

Managing a network is a matter of scale. Providing a policy for administrative access to network devices depends directly on the size of the network and the number of administrators required to maintain the network. Local authentication on a network device can be performed, but it is not scalable. The use of network management tools can help in large networks, but if local authentication is used on each network device, the policy usually consists of a single login on the network device. This does not promote adequate network device security. Using Cisco Secure ACS allows a centralized administrator database, and administrators can be added or deleted at one location. TACACS+ is the recommended AAA protocol for controlling AAA client administrative access because of its ability to provide per-command control (command authorization) of a AAA client administrator's access to the device. RADIUS is not well-suited for this purpose because of the one-time transfer of authorization information at time of initial authentication.

Downloaded from www.Manualslib.com manuals search engine

The type of access is also an important consideration. If there are to be different administrative access levels to the AAA clients, or if a subset of administrators is to be limited to certain systems, Cisco Secure ACS can be used with command authorization per network device to restrict network administrators as necessary. To use local authentication restricts the administrative access policy to no login on a device or using privilege levels to control access. Controlling access by means of privilege levels is cumbersome and not very scalable. This requires that the privilege levels of specific commands are altered on the AAA client device and specific privilege levels are defined for the user login. It is also very easy to create more problems by editing command privilege levels. Using command authorization on Cisco Secure ACS doesn't require that you alter the privilege level of controlled commands. The AAA client sends the command to Cisco Secure ACS to be parsed and Cisco Secure ACS determines whether the administrator has permission to use the command. The use of AAA allows authentication on any AAA client to any user on Cisco Secure ACS and facilitates the limitation of access to these devices on a per-AAA client basis.

A small network with a small number of network devices may require only one or two individuals to administer it. Local authentication on the device is usually sufficient. If you require more granular control than that which authentication can provide, some means of authorization is necessary. As discussed earlier, controlling access using privilege levels can be cumbersome. Cisco Secure ACS reduces this problem.

In large enterprise networks, with many devices to administer, the use of Cisco Secure ACS becomes a practical necessity. Because administration of many devices requires a larger number of network administrators, with varying levels of access, the use of local control is simply not a viable way of keeping track of network device configuration changes required when changing administrators or devices. The use of network management tools, such as CiscoWorks2000, helps to ease this burden, but maintaining security is still an issue. Because Cisco Secure ACS can comfortably handle up to 100,000 users, the number of network administrators that Cisco Secure ACS supports is rarely an issue. If there is a large remote access population using RADIUS for AAA support, the corporate IT team should consider separate TACACS+ authentication using Cisco Secure ACS for the administrative team. This would isolate the general user population from the administrative team and reduce the likelihood of inadvertent access to network devices. If this is not a suitable solution, using TACACS+ for administrative (shell/exec) logins, and RADIUS for remote network access, provides sufficient security for the network devices.

Downloaded from www.Manualslib.com manuals search engine

Separation of Administrative and General Users

It is important to keep the general network user from accessing network devices. Even though the general user may not have any intention to "hack the system," inadvertent access could easily cause accidental disruption to network access. Separation of the general user from the administrative user falls into the realm of AAA and Cisco Secure ACS.

The easiest, and recommended, method to perform such separation is to use RADIUS for the general remote access user and TACACS+ for the administrative user. An issue that arises is that an administrator may also require remote network access, like the general user. If you use Cisco Secure ACS this poses no problem. The administrator can have both RADIUS and TACACS+ configurations in Cisco Secure ACS. Using authorization, RADIUS users can have PPP (or other network access protocols) set as the permitted protocol. Under TACACS+, only the administrator would be configured to allow shell (exec) access.

For example, if the administrator is dialing into the network as a general user, a AAA client would use RADIUS as the authenticating/authorizing protocol and the PPP protocol would be authorized. In turn, if the same administrator remotely connects to a AAA client to make configuration changes, the AAA client would use the TACACS+ protocol for authentication/authorization. Because this administrator is configured on Cisco Secure ACS with permission for shell under TACACS+, he would be authorized to log in to that device. This does require that the AAA client have two separate configurations on Cisco Secure ACS, one for RADIUS and one for TACACS+. An example of a AAA client configuration under IOS that effectively separates PPP and shell logins follows:

```
aaa new-model
 tacacs-server host ip-address
 tacacs-server key secret-key
 radius-server host ip-address
 radius-server key secret-key
 aaa authentication ppp default group radius
 aaa authentication login default group tacacs+ local
 aaa authentication login console none
 aaa authorization network default group radius
 aaa authorization exec default group tacacs+ none
 aaa authorization command 15 default group tacacs+ none
 username user password password
 line con 0
 login authentication console
```


Downloaded from www.Manualslib.com manuals search engine

Conversely, if a general user attempts to use their remote access to log in to a network device, Cisco Secure ACS checks and approves the user's username and password, but the authorization process would fail because that user would not have credentials that allow shell/exec access to the device.

Database

Aside from topological considerations, the database is one of the most influential factors involved in making deployment decisions for Cisco Secure ACS. The size of the user base, distribution of users throughout the network, access requirements, and type of database employed all contribute to how Cisco Secure ACS is used.

Number of Users

Cisco Secure ACS is designed for the enterprise environment, comfortably handling 100,000 users. This is usually more than adequate for a corporation. In an environment that exceeds these numbers, the user base would typically be geographically dispersed, which lends itself to the use of more than one Cisco Secure ACS configuration. A WAN failure could render a local network inaccessible because of the loss of the authentication server. In addition to this issue, reducing the number of users that a single Cisco Secure ACS handles improves performance by lowering the number of logins occurring at any given time and by reducing the load on the database itself.

Type of Database

Cisco Secure ACS supports a number of database options. Under the current version, the options include using the CiscoSecure user database or using remote authentication via any of the external databases supported. For more information about database options, types, and features, see the "Authentication and User Databases" section on page 1-8, or Chapter 11, "Working with User Databases," or Chapter 12, "Administering External User Databases." Each database option has its own advantages and limitations in scalability and performance.

Downloaded from www.Manualslib.com manuals search engine

Network Speed and Reliability

Network speed, also referred to as network latency, and network reliability are also important factors in how Cisco Secure ACS is deployed. Delays in authentication can result in timeouts at the end user's client side or the AAA client.

The general rule for large, extended networks, such as a globally dispersed corporation, is to have at least one Cisco Secure ACS deployed in each region. This may not be adequate without a reliable, high-speed connection between sites. Many corporations are now using secure VPN connections between sites, using the Internet to provide the link. This saves time and money, but does not provide the speed and reliability that a dedicated frame relay or T1 link would provide. If authentication is critical to maintain business functionality, as in the case with a store having cash registers linked via a wireless LAN, the loss of the WAN connection to a remote Cisco Secure ACS could be catastrophic.

The same issue can be applied to an external database used by Cisco Secure ACS. The database should be deployed in proximity near enough to the Cisco Secure ACS installation to ensure reliable and timely access. Using a local Cisco Secure ACS with a remote database can result in the same problems as using a remote Cisco Secure ACS. Another possible problem in this scenario is that a user may experience timeout problems. The AAA client would be able to contact Cisco Secure ACS, but Cisco Secure ACS would wait for a reply from the external user database that might be delayed or never arrive. If the Cisco Secure ACS were remote, the AAA client would time out and try an alternative method to authenticate the user, but in the latter case it is likely the end user client would time out first.

Suggested Deployment Sequence

While there is no single, one-size-fits-all process for all Cisco Secure ACS deployments, you should consider following the sequence, keyed to the high-level functions represented in the navigation toolbar. Also bear in mind that many of these deployment activities are iterative in nature; you may find that you repeatedly return to such tasks as interface configuration as your deployment proceeds.

Downloaded from www.Manualslib.com manuals search engine

- **Configure Administrators**—You should configure at least one administrator at the outset of deployment; otherwise, there is not remote administrative access and all configuration activity must be done from the server. You should also have a detailed plan for establishing and maintaining an administrative policy.

  For more information about setting up administrators, see Chapter 10, "Setting Up and Managing Administrators and Policy."

- **Configure the Cisco Secure ACS HTML Interface—**You can configure Cisco Secure ACS HTML interface to show only those features and controls that you intend to use. This makes using Cisco Secure ACS less difficult than it would be if you had to contend with multiple parts of the HTML interface that you did not plan to use. The price of this convenience can sometimes be frustration that features and controls do not appear because you failed to configure them in the Interface Configuration section. For guidance on configuring the HTML interface, see the "Interface Design Concepts" section on page 3-2.

  For information about configuring particular aspects of the HTML interface, see the following sections of the interface configuration chapter:

  - User Data Configuration Options, page 3-3
  - Advanced Options, page 3-4
  - Protocol Configuration Options for TACACS+, page 3-7
  - Protocol Configuration Options for RADIUS, page 3-10

- **Configure System—**There are more than a dozen functions within the System Configuration section to be considered, from setting the format for the display of dates and password validation to configuring settings for database replication and RDBMS synchronization. These functions are detailed in Chapter 8, "Establishing Cisco Secure ACS System Configuration." Of particular note during initial system configuration is setting up the logs and reports to be generated by Cisco Secure ACS; for more information, see Chapter 9, "Working with Logging and Reports."

- **Configure Network—**You control distributed and proxied AAA functions in the Network Configuration section of the HTML interface. From here, you establish the identity, location, and grouping of AAA clients and servers, and determine what authentication protocols each is to employ. For more information, see Chapter 4, "Setting Up and Managing Network Configuration."

Downloaded from www.Manualslib.com manuals search engine

- **Configure External User Database**—During this phase of deployment you must decide whether and how you intend to implement an external database to establish and maintain user authentication accounts. Typically, this decision is made according to your existing network administration mechanisms. For information about the types of databases Cisco Secure ACS supports and instructions for establishing them, see Chapter 11, "Working with User Databases."

  Along with the decision to implement an external user database (or databases), you should have detailed plans that specify your requirements for Cisco Secure ACS database replication, backup, and synchronization. These aspects of configuring CiscoSecure user database management are detailed in Chapter 8, "Establishing Cisco Secure ACS System Configuration."

- **Configure Shared Profile Components—**With most aspects of network configuration already established and before configuring user groups, you should configure your Shared Profile Components. When you set up and name the network access restrictions and command authorization sets you intend to employ, you lay out an efficient basis for specifying user group and single user access privileges. For more information about Shared Profile Components, see the Chapter 5, "Setting Up and Managing Shared Profile Components."

- **Configure Groups—**Having previously configured any external user databases you intend to employ, and before configuring your user groups, you should decide how to implement two other Cisco Secure ACS features related to external user databases: unknown user processing and database group mapping. For more information see the "Unknown User Processing" section on page 12-1 and the "Database Group Mappings" section on page 12-10. Then, you are able to configure your user groups with a complete plan of how Cisco Secure ACS is to implement authorization and authentication. For more information, see the "Setting Up and Managing User Groups" section on page 6-1.

Downloaded from www.Manualslib.com manuals search engine

- **Configure Users**—With groups established, you can establish user accounts. It is useful to remember that a particular user can belong to only one user group, and that settings made at the user level override settings made at the group level. For more information, see the Chapter 7, "Setting Up and Managing User Accounts."
- **Configure Reports**—Using the Reports and Activities section of the Cisco Secure ACS HTML interface, you can specify the nature and scope of logging that Cisco Secure ACS performs. For more information, see Chapter 9, "Working with Logging and Reports."

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Setting Up the Cisco Secure ACS HTML Interface

Ease of use is the overriding design principle of the HTML interface in the Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS). Cisco Secure ACS presents intricate concepts of network security from the perspective of an administrator. The Interface Configuration section of Cisco Secure ACS enables you to configure the Cisco Secure ACS HTML interface—you can tailor the interface to simplify the screens you will use by hiding the features that you do not use and by adding fields for your specific configuration.

This chapter presents the details of configuring the Cisco Secure ACS interface through four topics:

- User Data Configuration Options, page 3-3
- Advanced Options, page 3-4
- Protocol Configuration Options for TACACS+, page 3-7
- Protocol Configuration Options for RADIUS, page 3-10

While it is logical to begin your Cisco Secure ACS configuration efforts here—configuring the interface—we also recommend that you return to this section to review and confirm your initial settings. Sometimes a section of the HTML interface that you initially believed should be hidden from view may later require configuration from within this section.

Downloaded from www.Manualslib.com manuals search engine

Tip If a section of the Cisco Secure ACS HTML interface appears to be "missing" or "broken" return to the Interface Configuration section and confirm that the particular section has been activated.

Interface Design Concepts

Before you begin to configure the Cisco Secure ACS HTML interface for your particular configuration, it is helpful to understand a few basic precepts of the system's operation. The information in the following sections is necessary for effective interface configuration.

User-to-Group Relationship

A user can belong to only one group at a time. As long as there are no conflicting attributes, users inherit group settings.

Note If a user profile has an attribute configured differently from the same attribute in the group profile, the user setting always overrides the group setting.

If a user has a unique configuration requirement, you can make that user a part of a group and set unique requirements on the User Setup page, or you can assign that user to his or her own group.

Per-User or Per-Group Features

You can configure most features at both group and user levels, with the following exceptions:

- **User level only**—Static IP address, password, and expiration
- **Group level only**—Password aging and time-of-day/day-of-week restrictions

Downloaded from www.Manualslib.com manuals search engine

User Data Configuration Options

The Configure User Defined Fields page enables you to add (or edit) up to five fields for recording information on each user. The fields you define in this section subsequently appear in the Supplementary User Information section at the top of the User Setup page. For example, you could add the user's company name, telephone number, department, billing code, and so on. You can also include these fields in the accounting logs. For more information about the accounting logs, see the "About Cisco Secure ACS Logs and Reports" section on page 9-4. For information on the data fields that comprise these options, see the "User-Defined Attributes" section on page G-34.

Defining New User Data Fields

To configure new user data fields, follow these steps:

Step 1 Click **Interface Configuration** and then click **User Data Configuration**.

Result: The Configure User Defined Fields page appears. Check boxes in the Display column indicate which fields are configured to appear in the Supplementary User Information section at the top of the User Setup page.

Step 2 Select a check box in the Display column.

Step 3 In the corresponding Field Title box, type a title for the new field.

Step 4 To configure another field, repeat step 2 and step 3.

Step 5 When you have finished configuring new user data fields, click **Submit**.

Tip You can change the title of a field by editing the text in the Field Title box and then clicking Submit.

Downloaded from www.Manualslib.com manuals search engine

Advanced Options

This feature enables you to determine which advanced features Cisco Secure ACS displays. You can simplify the pages displayed in other areas of the Cisco Secure ACS HTML interface by hiding advanced features that you do not use. Many of these options do not appear if they are not enabled.

Caution Disabling an advanced option in the Interface Configuration section does not affect anything except the display of that function in the CSACS HTML interface. Settings made while an advanced option was active (selected) remain in effect when that advanced option is no longer displayed in the interface (de-selected). Further, the interface displays any advanced option that is enabled or has non-default values, even if you have configured that advanced option to be hidden. If you later disable the option or delete its value, Cisco Secure ACS hides the advanced option.

The advanced option features include the following:

- **Per-User TACACS+/RADIUS Attributes**—When selected, this feature enables TACACS+/RADIUS attributes to be set at a per-user level, in addition to being set at the group level.
- **User-Level Network Access Restriction Sets**—When selected, this feature enables the Shared Profile Component network access restrictions (NARs) options on the User Setup page. These options allow you to apply previously configured, named, IP-based and CLID/DNIS-based NARs at the user level. For information on defining a NAR, or NAR set, within Shared Profile Components, see the "Shared Network Access Restrictions Configuration" section on page 5-7.
- **User-Level Network Access Restrictions**—When selected, this feature enables the two sets of options for defining user-level, IP-based and CLI/DNIS-based NARs on the User Setup page.
- **User-Level Downloadable ACLs**—When selected, this feature enables the Downloadable ACLs section on the User Setup page.
- **Default Time-of-Day/Day-of-Week Specification**—When selected, this feature enables the default time-of-day/day-of-week access settings grid on the Group Setup page.

Downloaded from www.Manualslib.com manuals search engine

- **Group-Level Network Access Restriction Sets**—When selected, this feature enables the Shared Profile Component NAR options on the Group Setup page. These options allow you to apply previously configured, named, IP-based and CLID/DNIS-based NARs at the group level. For information on defining a NAR, or NAR set, within Shared Profile Components, see the "Shared Network Access Restrictions Configuration" section on page 5-7.
- **Group-Level Network Access Restrictions**—When selected, this feature enables the two sets of options for defining group-level, IP-based and CLI/DNIS-based NARs on the on the Group Setup page.
- **Group-Level Downloadable ACLs**—When selected, this feature enables the Downloadable ACLs section on the Group Setup page.
- **Group-Level Password Aging**—When selected, this feature enables the Password Aging section on the Group Setup page. The Password Aging feature enables you to force users to change their passwords.
- **Max Sessions**—When selected, this feature enables the Max Sessions section on the User Setup and Group Setup pages. The Max Sessions option sets the maximum number of simultaneous connections for a group or a user.
- **Usage Quotas**—When selected, this feature enables the Usage Quotas sections on the User Setup and Group Setup pages. The Usage Quotas option sets one or more quotas for usage by a group or a user.
- **Distributed System Settings**—When selected, this feature displays the AAA server and proxy table on the Network Interface page. If the tables are not empty and have information other than the defaults in them, they always appear.
- **Remote Logging**—When selected, this feature enables the Remote Logging feature in the Logging page of the System Configuration section.
- **Cisco Secure ACS Database Replication**—When selected, this feature enables the Cisco Secure ACS database replication information on the System Configuration page.
- **RDBMS Synchronization**—When selected, this feature enables the RDBMS (Relational Database Management System) Synchronization option on the System Configuration page. If RDBMS Synchronization is configured, this option always appears.
- **IP Pools**—When selected, this feature enables the IP Pools Address Recovery and IP Pools Server options on the System Configuration page.

Downloaded from www.Manualslib.com manuals search engine

- **Network Device Groups**—When selected, this option enables network device groups (NDGs). When NDGs are enabled, the Network Configuration section and parts of the User Setup and Group Setup pages change to enable you to manage groups of network devices (AAA clients or AAA servers). This feature is useful if you have many devices to administer.
- **Voice over IP (VoIP) Group Settings**—When selected, this feature enables the VoIP option on the Group Setup page.
- **Voice-over-IP (VoIP) Accounting Configuration**—When selected, this feature enables the VoIP Accounting Configuration option on the System Configuration page. This option is used to determine the logging format of RADIUS VoIP accounting packets.
- **ODBC Logging**—When selected, this feature enables the ODBC logging sections on the Logging page of the System Configuration section.

Setting Advanced Options for the Cisco Secure ACS User Interface

To set advanced options for the Cisco Secure ACS HTML interface, follow these steps:

Step 1 Click **Interface Configuration**.

Step 2 Click **Advanced Options**.

Result: The Advanced Options table appears.

Step 3 Select each option that you want displayed (enabled) in the Cisco Secure ACS HTML interface.

Caution Disabling an advanced option in the Interface Configuration section does not affect anything except the display of that function in the Cisco Secure ACS interface. Settings made while an advanced option was active (selected) remain in effect when that advanced option is no longer displayed in the interface (de-selected).

Downloaded from www.Manualslib.com manuals search engine

Step 4 When you have finished making selections, click **Submit**.

Result: Cisco Secure ACS alters the contents of various sections of the HTML interface according to the selections made.

Protocol Configuration Options for TACACS+

The TACACS+ (Cisco) section details the configuration of the Cisco Secure ACS HTML interface for TACACS+ settings. The interface settings enable you to display or hide TACACS+ administrative and accounting options. You can simplify the HTML interface by hiding the features that you do not use.

The TACACS+ (Cisco) section comprises three distinct areas, as follows:

Tip The default interface setting presents a single column of check boxes, at the group level only, for selecting TACACS+ Services Settings and New Service Settings. To view two columns of check boxes that enable you to configure settings at the Group level or the User level, you must have enabled the Per-user TACACS+/RADIUS Attributes option on the Advanced Options page of Interface Configuration section.

- **TACACS+ Services Settings**—In this area is a list of the most commonly used services and protocols for TACACS+. You select each TACACS+ service that you want to appear as a configurable option on either the User Setup page or Group Setup page.
- **New Services**—In this area you can enter any services or protocols particular to your network configuration.
- **Advanced Configuration Options**—In this area you can add more detailed information for even more tailored configurations.

Downloaded from www.Manualslib.com manuals search engine

The four items you can choose to hide or display are as follows:

- **Advanced TACACS+ Features**—This option displays or hides the Advanced TACACS+ Options section on the User Setup page. These options include Privilege Level Authentication and Outbound Password Configuration for SENDPASS and SENDAUTH clients, such as routers.
- **Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day settings**—If this option is selected, a grid appears on the User Setup page that enables you to override the TACACS+ scheduling attributes on the Group Setup page.

  You can control the use of each TACACS+ service by the time of day and day of week. For example, you can restrict Exec (Telnet) access to business hours but permit PPP-IP access at any time.

  The default setting is to control time-of-day access for all services as part of authentication. However, you can override the default and display a time-of-day access grid for every service. This keeps user and group setup easy to manage, while making this feature available for the most sophisticated environments. This feature applies only to TACACS+ because TACACS+ can separate the authentication and authorization processes. RADIUS time-of-day access applies to all services. If both TACACS+ and RADIUS are used simultaneously, the default time-of-day access applies to both. This provides a common method to control access regardless of the access control protocol.
- **Display a window for each service selected in which you can enter customized TACACS+ attributes**—If this option is selected, an area appears on the User Setup and Group Setup pages that enables you to enter custom TACACS+ attributes.

  Cisco Secure ACS can also display a custom command field for each service. This text field enables you to make specialized configurations to be downloaded for a particular service for users in a particular group.

Downloaded from www.Manualslib.com manuals search engine

You can use this feature to send many TACACS+ commands to the access device for the service, provided that the device supports the command, and that the command syntax is correct. This feature is disabled by default, but you can enable it the same way you enable attributes and time-of-day access.

– **Display enable Default (Undefined) Service Configuration**—If this check box is selected, an area appears on the User Setup and Group Setup pages that enables you to permit unknown TACACS+ services, such as CDP.

Note This option should be used by advanced system administrators only.

Note Customized settings at the user level take precedence over settings at the group level.

Setting Options for TACACS+

This procedure enables you to display or hide TACACS+ administrative and accounting options. It is unlikely that you will use every service and protocol available for TACACS+. Displaying each would make setting up a user or group cumbersome. To simplify setup, you can use the TACACS+ (Cisco IOS) Edit page to customize the services and protocols that appear.

To configure the user interface for TACACS+ options, follow these steps:

Note The Cisco Secure ACS HTML interface displays any protocol option that is enabled or has non-default values, even if you have configured that protocol option to be hidden. This behavior prevents Cisco Secure ACS from hiding active settings. If you later disable the option or delete its value, Cisco Secure ACS hides the protocol option.

Step 1 Click **Interface Configuration**.

Step 2 Click **TACACS+ (Cisco IOS)**.

Downloaded from www.Manualslib.com manuals search engine

Result: The TACACS+ (Cisco) page of the Interface Configuration section appears.

Step 3 In the TACACS+ Services table, select the check box for each TACACS+ service you want displayed on the applicable setup page.

Step 4 To add new services and protocols, follow these steps:

a. In the New Services section of the TACACS+ Services table, type in any Service and Protocol to be added.

b. Select the appropriate check box to select those that should be displayed for configuration either under User Setup, or Group Setup, or both.

Step 5 In the Advanced Configurations Options section, select the check boxes of the display options you want to enable.

Step 6 When you have finished setting TACACS+ interface display options, click **Submit**.

Result: The selections made in this procedure determine what TACACS+ options Cisco Secure ACS displays in other sections of the HTML interface.

Protocol Configuration Options for RADIUS

This section details the configuration of the Cisco Secure ACS HTML interface for RADIUS settings. The interface settings enable you to display or hide various RADIUS administrative and accounting options. You can simplify the HTML interface by hiding the features that you do not use.

Provided that you have the corresponding AAA clients configured, the User Interface section displays the following RADIUS protocol configuration selections:

- **(IETF) RADIUS Settings**—This page lists all attributes available for (IETF) RADIUS.

  These standard (IETF) RADIUS attributes are available for any network device configuration when using RADIUS. If you want to use IETF attribute number 26, the vendor-specific attribute (VSA), select Interface Configuration and then RADIUS for the vendors whose network devices you

Downloaded from www.Manualslib.com manuals search engine

use. Attributes for (IETF) RADIUS and the VSA for each RADIUS network device vendor supported by Cisco Secure ACS appear in User Setup or Group Setup.

Note The RADIUS (IETF) attributes are shared with RADIUS VSAs. You must configure the first RADIUS attributes from RADIUS (IETF) for the RADIUS vendor.

The Tags to Display Per Attribute option (located under Advanced Configuration Options) enables you to specify how many values to display for tagged attributes on the User Setup and Group Setup pages. Examples of tagged attributes include [064]Tunnel-Type and [069]Tunnel-Password.

For detailed procedural information, see the "Setting Protocol Configuration Options for (IETF) RADIUS" section on page 3-12.

- **RADIUS (Cisco IOS/PIX) Settings**—This section allows you to enable the specific attributes for RADIUS (Cisco IOS/PIX). For detailed procedural information, see the "Setting Protocol Configuration Options for RADIUS (Cisco IOS/PIX)" section on page 3-14.
- **RADIUS (Ascend) Settings**—This section allows you to enable the RADIUS vendor-specific attributes for RADIUS (Ascend). For detailed procedures, see the "Setting Protocol Configuration Options for RADIUS (Ascend)" section on page 3-14.
- **RADIUS (Cisco VPN 3000) Settings**—This section allows you to enable the RADIUS vendor-specific attributes for RADIUS (Cisco VPN 3000). For detailed procedures, see the "Setting Protocol Configuration Options for RADIUS (Cisco VPN 3000)" section on page 3-15.
- **RADIUS (Cisco VPN 5000) Settings**—This section allows you to enable the RADIUS vendor-specific attributes for RADIUS (Cisco VPN 5000). For detailed procedures, see the "Setting Protocol Configuration Options for RADIUS (Cisco VPN 5000)" section on page 3-16.
- **RADIUS (Microsoft) Settings**—This section allows you to enable the RADIUS vendor-specific attributes for RADIUS (Microsoft). For detailed procedures, see the "Setting Protocol Configuration Options for RADIUS (Microsoft)" section on page 3-17.

Downloaded from www.Manualslib.com manuals search engine

- **RADIUS (Nortel) Settings**—This section allows you to enable the RADIUS vendor-specific attributes for RADIUS (Nortel). For detailed procedures, see the "Setting Protocol Configuration Options for RADIUS (Nortel)" section on page 3-18.
- **RADIUS (Juniper) Settings**—This section allows you to enable the RADIUS vendor-specific attributes for RADIUS (Juniper). For detailed procedures, see the "Setting Protocol Configuration Options for RADIUS (Juniper)" section on page 3-19.
- **RADIUS (Cisco BBSM) Settings**—This section allows you to enable the RADIUS vendor-specific attributes for RADIUS (Cisco BBSM). For detailed procedures, see the "Setting Protocol Configuration Options for RADIUS (Cisco BBSM)" section on page 3-20.

While Cisco Secure ACS ships with these listed VSAs prepackaged, it also enables you to define and configure custom attributes for any VSA set not already contained in Cisco Secure ACS. If you have configured a custom VSA and a corresponding AAA client, from the Interface Configuration section you can select the custom VSA and then set the options for how particular attributes appear as configurable options on the User Setup or Group Setup page. For information about creating user-defined RADIUS VSAs, see the "User-Defined RADIUS Vendors and VSA Sets" section on page E-27.

Radius (Cisco Aironet) is not listed in Internet Configuration because there is no configuration required.

Setting Protocol Configuration Options for (IETF) RADIUS

This procedure enables you to hide or display any of the standard (IETF) RADIUS attributes for configuration from other portions of the Cisco Secure ACS HTML interface.

Note If the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options is selected, a User check box appears alongside the Group check box for each attribute.

Downloaded from www.Manualslib.com manuals search engine

Note Each selected IETF RADIUS attribute must be supported by all network devices using RADIUS.

To set protocol configuration options for (IETF) RADIUS attributes, follow these steps:

Step 1 Click **Interface Configuration**.

Step 2 Click **RADIUS (IETF)**.

Result: The RADIUS (IETF) page appears.

Step 3 For each IETF RADIUS attribute that you want to appear as a configurable option on the User Setup or Group Setup page, select the corresponding check box.

Note Each attribute selected must be supported by your RADIUS network devices.

Note Attributes marked "*" are sent from the AAA client to the RADIUS server and hence cannot be configured in the RADIUS setup screens.

Step 4 To specify how many values to display for tagged attributes on the User Setup and Group Setup pages, select the **Tags to Display Per Attribute** option, and then select a value from the corresponding list. Examples of tagged attributes are [064] Tunnel-Type and [069] Tunnel-Password.

Step 5 When you have finished selecting the attributes, click **Submit** at the bottom of the page.

Result: Each IETF RADIUS attribute that you selected appears as a configurable option on the User Setup or Group Setup page, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Setting Protocol Configuration Options for RADIUS (Cisco IOS/PIX)

This procedure allows you to enable the Cisco IOS/PIX RADIUS VSA. Selecting this attribute displays an entry field under User Setup and/or Group Setup in which any TACACS+ commands can be entered to fully leverage TACACS+ in a RADIUS environment.

Note If the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options is selected, a User check box appears alongside the Group check box for each attribute.

To set protocol configuration options for the Cisco RADIUS attribute follow these steps:

Step 1 Click **Interface Configuration**.

Step 2 Click **RADIUS (Cisco IOS/PIX)**.

Result: The RADIUS (Cisco IOS/PIX) page appears.

Step 3 Select the check box for either **User** or **Group**, or both, next to attribute number 26, the VSA for Cisco.

Step 4 Click **Submit** at the bottom of the page.

Result: According to your selections, the attribute for the Cisco RADIUS VSA appears on the User Setup or Group Setup pages, or both, as a configurable option with a field in which you can enter TACACS+ commands.

Setting Protocol Configuration Options for RADIUS (Ascend)

This procedure enables you to hide or display RADIUS (Ascend) attributes for configuration from other portions of the Cisco Secure ACS HTML interface.

Downloaded from www.Manualslib.com manuals search engine

Note If the Per-user TACACS+/RADIUS Attributes check box on the Advanced Options page of Interface Configuration is selected, a User check box appears alongside the Group check box for each attribute.

To set protocol configuration options for RADIUS (Ascend) attributes, follow these steps:

Step 1 Click **Interface Configuration**.

Step 2 Click **RADIUS (Ascend)**.

Result: The Edit RADIUS (Ascend) page appears, listing extended attributes.

Step 3 For each RADIUS (Ascend) attribute that you want to appear as a configurable option on the User Setup or Group Setup page, select the corresponding check box.

Note Each attribute selected must be supported by your RADIUS network devices.

Step 4 Click **Submit** at the bottom of the page.

Setting Protocol Configuration Options for RADIUS (Cisco VPN 3000)

This procedure enables you to hide or display RADIUS (Cisco VPN 3000 Concentrator) attributes for configuration from other portions of the Cisco Secure ACS HTML interface.

The RADIUS (Cisco VPN 3000 Concentrator) page lists all the attributes available for Cisco VPN 3000 Concentrator RADIUS.

Note If the Per-user TACACS+/RADIUS Attributes check box on the Advanced Options page of Interface Configuration is selected, a User check box appears alongside the Group check box for each attribute.

Downloaded from www.Manualslib.com manuals search engine

To set protocol configuration options for RADIUS (Cisco VPN 3000) attributes, follow these steps:

Step 1 Click **Interface Configuration**.

Step 2 Click **RADIUS (Cisco VPN 3000)**.

Result: The RADIUS (Cisco VPN 3000 Concentrator) edit page appears.

Step 3 Select the check box for either **User** or **Group**, or both, for each RADIUS (Cisco VPN 3000) service you want to appear as a configurable option on the User Setup or Group Setup page.

Note Each attribute selected must be supported by the Cisco VPN 3000 Concentrator RADIUS network devices.

Step 4 When you have finished selecting the attributes, click **Submit** at the bottom of the page.

Setting Protocol Configuration Options for RADIUS (Cisco VPN 5000)

This procedure enables you to hide or display RADIUS (Cisco VPN 5000 Concentrator) attributes for configuration from other portions of the Cisco Secure ACS HTML interface.

The RADIUS (Cisco VPN 5000 Concentrator) page lists all the attributes available for Cisco VPN 5000 Concentrator RADIUS.

Note If the Per-user TACACS+/RADIUS Attributes check box on the Advanced Options page of Interface Configuration is selected, a User check box appears alongside the Group check box for each attribute.

Downloaded from www.Manualslib.com manuals search engine

To set protocol configuration options for RADIUS (Cisco VPN 5000) attributes, follow these steps:

Step 1 Click **Interface Configuration**.

Step 2 Click **RADIUS (Cisco VPN 5000)**.

Result: The RADIUS (Cisco VPN 3000 Concentrator) edit page appears.

Step 3 Select the check box for either **User** or **Group**, or both, for each RADIUS (Cisco VPN 5000) service you want to appear as a configurable option on the User Setup or Group Setup page.

Note Each attribute selected must be supported by the Cisco VPN 5000 Concentrator RADIUS network devices.

Step 4 Click **Submit** at the bottom of the page.

Setting Protocol Configuration Options for RADIUS (Microsoft)

This procedure enables you to hide or display RADIUS (Microsoft) attributes for configuration from other portions of the Cisco Secure ACS HTML interface.

The RADIUS (Microsoft) page lists all the attributes available for Microsoft RADIUS.

Note If the Per-user TACACS+/RADIUS Attributes check box on the Advanced Options page of Interface Configuration is selected, a User check box appears alongside the Group check box for each attribute.

To set protocol configuration options for RADIUS (Microsoft) attributes, follow these steps:

Step 1 Click **Interface Configuration**.

Step 2 Click **RADIUS (Microsoft)**.

Result: The RADIUS (Microsoft) edit page appears.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select the check box for either **User** or **Group**, or both, for each RADIUS (Microsoft) service you want to appear as a configurable option on the User Setup or Group Setup page.

Note Each attribute selected must be supported by the Microsoft RADIUS VSA.

Step 4 Click **Submit** at the bottom of the page.

Setting Protocol Configuration Options for RADIUS (Nortel)

This procedure enables you to hide or display RADIUS (Nortel) attributes for configuration from other portions of the Cisco Secure ACS HTML interface.

The RADIUS (Nortel) page lists all the attributes available for Nortel RADIUS.

Note If the Per-user TACACS+/RADIUS Attributes check box on the Advanced Options page of Interface Configuration is selected, a User check box appears alongside the Group check box for each attribute.

To set protocol configuration options for RADIUS (Nortel) attributes, follow these steps:

Step 1 Click **Interface Configuration**.

Step 2 Click **RADIUS (Nortel)**.

Result: The RADIUS (Nortel) edit page appears.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select the check box for either **User** or **Group**, or both, for each RADIUS (Nortel) service you want to appear as a configurable option on the User Setup or Group Setup page.

Note Each attribute selected must be supported by the Nortel RADIUS VSA.

Step 4 Click **Submit** at the bottom of the page.

Setting Protocol Configuration Options for RADIUS (Juniper)

This procedure enables you to hide or display RADIUS (Juniper) attributes for configuration from other portions of the Cisco Secure ACS HTML interface.

The RADIUS (Juniper) page lists all the attributes available for Juniper RADIUS.

Note If the Per-user TACACS+/RADIUS Attributes check box on the Advanced Options page of Interface Configuration is selected, a User check box appears alongside the Group check box for each attribute.

To set protocol configuration options for RADIUS (Juniper) attributes, follow these steps:

Step 1 Click **Interface Configuration**.

Step 2 Click **RADIUS (Juniper)**.

Result: The RADIUS (Juniper) edit page appears.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select the check box for either **User** or **Group**, or both, for each RADIUS (Juniper) service you want to appear as a configurable option on the User Setup or Group Setup page.

Note Each attribute selected must be supported by the Juniper RADIUS VSA.

Step 4 Click **Submit** at the bottom of the page.

Setting Protocol Configuration Options for RADIUS (Cisco BBSM)

This procedure enables you to hide or display the RADIUS (Cisco BBSM) attribute for configuration from other portions of the Cisco Secure ACS HTML interface.

The RADIUS (Cisco BBSM) page lists the attribute available for Building Broadband Service Manger (BBSM) RADIUS.

Note If the Per-user TACACS+/RADIUS Attributes check box on the Advanced Options page of Interface Configuration is selected, a User check box appears alongside the Group check box for each attribute.

To set protocol configuration options for RADIUS (Cisco BBSM) attributes, follow these steps:

Step 1 Click **Interface Configuration**.

Step 2 Click **RADIUS (Cisco BBSM)**.

Result: The RADIUS (Cisco BBSM) edit page appears.

Step 3 Select the check box for either **User** or **Group**, or both, for the service you want to appear as a configurable option on the User Setup or Group Setup page.

Step 4 Click **Submit** at the bottom of the page.

Downloaded from www.Manualslib.com manuals search engine

Setting Up and Managing Network Configuration

This chapter details concepts and procedures for configuring the Cisco Secure ACS network and establishing a distributed system.

The appearance of the opening page you see when you click Network Configuration differs according to the network configuration selections you've made in the Interface Configuration section. The four tables that may appear in this section are as follows:

- **AAA Clients**—This table lists each AAA client that is configured on the network, together with its IP address and associated protocol.

  If you are using network device groups (NDGs), this table does not appear on the initial page, but is accessed through the Network Device Group table. For more information about this interface configuration, see the "Advanced Options" section on page 3-4.

- **AAA Servers**—This table lists each AAA server that is configured on the network together with its IP Address and associated type.

  This table does not appear unless you have enabled the Distributed System Settings feature in Interface Configuration.

  If you are using NDGs, this table does not appear on the initial page, but is accessed through the Network Device Groups table. For more information about this interface configuration, see the "Advanced Options" section on page 3-4.

Downloaded from www.Manualslib.com manuals search engine

- **Network Device Groups**—This table lists the name of each NDG that has been configured, and the number of AAA clients and AAA servers assigned to each NDG. If you are using NDGs, the AAA Clients table and AAA Servers table do not appear on the opening page. To configure a AAA client or AAA server, you must click the name of the NDG to which the device is assigned. If the newly configured device is not assigned to an NDG, it automatically belongs to the (Not Assigned) group.

  This table appears only when you have configured the interface to use NDGs. For more information about this interface configuration, see the "Advanced Options" section on page 3-4.

- **Proxy Distribution Table**—You can use the Proxy Distribution Table to configure proxy capabilities including "domain" stripping. For more information, see the "Proxy Distribution Table Configuration" section on page 4-25.

  This table appears only when you have configured the interface to enable Distributed Systems Settings. For more information about this interface configuration, see the "Advanced Options" section on page 3-4.

This chapter includes sections that provide the concepts and procedures related to each of these tables, as follows:

- AAA Client Configuration, page 4-8
- AAA Server Configuration, page 4-15
- Network Device Group Configuration, page 4-20
- Proxy Distribution Table Configuration, page 4-25

About Distributed Systems

Cisco Secure ACS can be used in a distributed system; that is, multiple Cisco Secure ACS servers and authentication, authorization, and accounting (AAA) servers can be configured to communicate with one another as primary, backup, client, or peer systems. This enables you to use powerful features such as the following:

- Proxy
- Fallback on failed connection

Downloaded from www.Manualslib.com manuals search engine

- CiscoSecure database replication
- Remote and centralized logging

AAA Servers in Distributed Systems

"AAA server" is the generic term for an access control server (ACS), and the two terms are often used interchangeably. AAA servers are used to determine who can access the network and what services are authorized for each user. The AAA server stores a profile containing authentication and authorization information for each user. Authentication information validates user identity, and authorization information determines what network services a user is permitted to use. A single AAA server can provide concurrent AAA services to many dial-up access servers, routers, and firewalls. Each network device can be configured to communicate with a AAA server. This makes it possible to centrally control dial-up access, as well as to secure network devices from unauthorized access.

These types of access control have unique authentication and authorization requirements. With Cisco Secure ACS, system administrators can use a variety of authentication methods that are used with different degrees of authorization privileges.

Completing the AAA functionality, Cisco Secure ACS serves as a central repository for accounting information. Each user session granted by Cisco Secure ACS can be fully accounted for, and its accounting information can be stored in the server. This accounting information can be used for billing, capacity planning, and security audits.

Note If the fields mentioned in this section do not appear in your Cisco Secure ACS HTML interface, enable them by clicking **Interface Configuration**, clicking **Advanced Options**, and then selecting the **Distributed System Settings** check box.

Default Distributed System Settings

You use both the AAA Servers table and the Proxy Distribution Table to establish distributed system settings. The parameters configured within these tables create the foundation to enable multiple Cisco Secure ACS servers to be configured to

Downloaded from www.Manualslib.com manuals search engine

work with one another. Each table contains a Cisco Secure ACS entry for itself. In the AAA Servers table, the only AAA server initially listed is itself; the Proxy Distribution Table lists an initial entry of (Default), which displays how the local Cisco Secure ACS is configured to handle each authentication request locally.

You can configure additional AAA servers in the AAA Servers table. This enables these devices to become available in the HTML interface so that they can be configured for other distributed features such as proxy, CiscoSecure user database replication, remote logging, and RDBMS synchronization. For information about configuring additional AAA servers, see the "Adding and Configuring a AAA Server" section on page 4-16.

Proxy in Distributed Systems

Proxy is a powerful feature that enables you to use Cisco Secure ACS for authentication in a network that uses more than one AAA server. Using proxy, Cisco Secure ACS automatically forwards an authentication request from a AAA client to another AAA server. After the request has been successfully authenticated, the authorization privileges that have been configured for the user on the remote AAA server are passed back to the original Cisco Secure ACS, where the AAA client applies the user's profile information for that session.

Proxy is useful in the provision of service to users, such as business travelers, who dial in to a network device other than the one they normally use and would otherwise be authenticated by a "foreign" AAA server. To use proxy, you must first click **Interface Configuration**, click **Advanced Options**, and then select the **Distributed System Settings** check box.

Whether, and where, an authentication request is to be forwarded is defined in the Proxy Distribution Table on the Network Configuration page. You can use multiple Cisco Secure ACS servers throughout your network. For information about configuring the Proxy Distribution Table, see the "Proxy Distribution Table Configuration" section on page 4-25.

Cisco Secure ACS employs character strings defined by the administrator to determine whether an authentication request should be processed locally or forwarded, and to where. When an end user dials in to the network device and Cisco Secure ACS finds a match for the character string defined in the Proxy Distribution Table, Cisco Secure ACS forwards the authentication request to the associated remote AAA server.

Downloaded from www.Manualslib.com manuals search engine

Note When a Cisco Secure ACS receives a TACACS+ authentication request forwarded by proxy, any Network Access Restrictions for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

Note In a network that uses more than one type of RADIUS protocol, Cisco Secure ACS accepts only IETF attributes. All other attributes, such as proprietary attributes, are not interpreted. If the AAA protocol for RADIUS is configured uniformly with the same attributes, all attributes are recognized.

For example, a Cisco Secure ACS receives an authentication request for mary.smith@corporate.com, where "@corporate.com" is a character string defined in the server's distribution table as being associated with another specific AAA server. The Cisco Secure ACS server receiving the authentication request for mary.smith@corporate.com then forwards the request to the AAA server with which the character string is associated. The entry in the Proxy Distribution Table defines the association.

Administrators with geographically dispersed networks can configure and manage the user profiles of employees within their immediate location or building. This enables the administrator to manage the policies of just their users and allows all authentication requests from other users within the company to be forwarded to their respective AAA server for authentication. Not every user profile needs to reside on every AAA server. This saves administration time and server space, and facilitates end users receiving the same privileges regardless of which access device they connect through.

Fallback on Failed Connection

You can configure the order in which Cisco Secure ACS checks remote AAA servers upon the failure of the network connection to the primary AAA server. If an authentication request cannot be sent to the first listed server, because of a network failure for example, the next listed server is checked. This continues, in order, down the list until a AAA server handles the authentication

Downloaded from www.Manualslib.com manuals search engine

request. If Cisco Secure ACS cannot connect to any server in the list, authentication fails. Failed connections are detected by failure of the nominated server to respond within a specified time period. That is, the request is timed out.

Character String

Cisco Secure ACS forwards authentication requests using a configurable set of characters with a delimiter, such as dots (.), slashes (/), backslashes (\), and hyphens (-). When configuring the Cisco Secure ACS character string to match, you must specify whether the character string is the prefix or suffix. For example, you can use “domain.us” as a suffix character string in username*domain.us, where * represents any delimiter. An example of a prefix character string is domain*username, where the * would be used to detect the “\” character.

Stripping

Stripping allows Cisco Secure ACS to remove, or strip, the matched character string from the username. When you enable stripping, Cisco Secure ACS examines each authentication request for matching information. When Cisco Secure ACS finds a match by character string in the Proxy Distribution Table, as described above, Cisco Secure ACS strips off the character string if you have configured it to do so. For example, in the proxy example that follows, the character string that accompanies the username establishes the ability to forward the request to another AAA server. If the user must enter the user ID of mary@corporate.com to be forwarded correctly to the AAA server for authentication, Cisco Secure ACS might find a match on the “@corporate.com” character string, and strip the “@corporate.com”, leaving a username of just “mary” which may be the username format that the destination AAA Server requires to identify the correct entry in its database.

Proxy in an Enterprise

This section presents a scenario of proxy used in an enterprise system. Mary is an employee with an office in the corporate headquarters in Los Angeles. Her username is mary@la.corporate.com. When Mary needs access to the network, she accesses the network locally and authenticates her username and password. Because Mary works in the Los Angeles office, her user profile, which defines her authentication and authorization privileges, resides on the local Los Angeles

Downloaded from www.Manualslib.com manuals search engine

AAA server. However, Mary occasionally travels to a division within the corporation in New York, where she still needs to access the corporate network to get her e-mail and other files. When Mary is in New York, she dials in to the New York office and logs in as mary@corporate.com. Her username is not recognized by the New York Cisco Secure ACS, but the Proxy Distribution Table contains an entry, "la", to forward the authentication request to the Los Angeles Cisco Secure ACS. Because Mary's username and password information reside on that AAA server, when she authenticates correctly, the authorization parameters assigned to her are applied by the AAA client in the New York office.

Remote Use of Accounting Packets

When proxy is employed, Cisco Secure ACS can dispatch AAA accounting packets in one of three ways:

- Log them locally
- Forward them to the destination AAA server
- Log them locally and forward copies to the destination AAA server

Sending accounting packets to the remote Cisco Secure ACS offers several benefits. When Cisco Secure ACS is configured to send accounting packets to the remote AAA server, the remote AAA server logs an entry in the accounting report for that session on the destination server. Cisco Secure ACS also caches the user's connection information and adds an entry in the List Logged on Users report. You can then view the information for users that are currently connected. Because the accounting information is being sent to the remote AAA server, even if the connection fails, you can view the Failed Attempts report to troubleshoot the failed connection.

Sending the accounting information to the remote AAA server also enables you to use the Max Sessions feature. The Max Sessions feature uses the Start and Stop records in the accounting packet. If the remote AAA server is a Cisco Secure ACS and the Max Sessions feature is implemented, you can track the number of sessions allowed for each user or group.

You can also choose to have Voice over IP (VoIP) accounting information logged remotely, either appended to the RADIUS Accounting log, in a separate VoIP Accounting log, or both.

Downloaded from www.Manualslib.com manuals search engine

Other Features Enabled by System Distribution

Beyond basic proxy and fallback features, configuring a Cisco Secure ACS to interact with distributed systems enables several other features that are beyond the scope of this chapter. These features include the following:

- **Replication**—For more information, see the "CiscoSecure Database Replication" section on page 8-6.
- **RDBMS synchronization**—For more information, see the "RDBMS Synchronization" section on page 8-24.
- **Remote and centralized logging**—For more information, see the "Remote Logging" section on page 9-29.

AAA Client Configuration

In this guide we use the term AAA client comprehensively to signify the device through which or to which service access is being attempted. This is the RADIUS or TACACS+ client device, and may comprise network access servers (NASes), PIX Firewalls, routers, or any other RADIUS or TACACS+ hardware/software client.

Details on working with AAA clients are given in the following three procedures:

- Adding and Configuring a AAA Client, page 4-9
- Editing an Existing AAA Client, page 4-12
- Deleting a AAA Client, page 4-14

Downloaded from www.Manualslib.com manuals search engine

Adding and Configuring a AAA Client

You can use this procedure to add and configure a AAA client.

To add a AAA client, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration section opens.

Step 2 Do one of the following:

a. If you are using NDGs, click the name of the NDG to which the AAA client is to be assigned. Then, click **Add Entry** below the AAA Clients table.

b. To add a AAA client when you have not enabled NDGs, click **Add Entry** below the AAA Clients table.

Result: The Add AAA Client page appears.

Step 3 In the AAA Client Hostname box, type the name assigned to this AAA client.

Note This field does not appear if you are configuring an existing AAA client.

Step 4 In the AAA Client IP Address box, type the AAA client's IP address or addresses.

Tip If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**. You can also use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.

Step 5 In the Key box, type the shared secret that the AAA client and Cisco Secure ACS use to encrypt the data.

Downloaded from www.Manualslib.com manuals search engine

Note For correct operation, the identical key must be configured on the AAA client and Cisco Secure ACS. Keys are case sensitive. Because the shared secrets are not synchronized in any way, it is easy to make mistakes when entering them upon both devices. Such mistakes will cause the AAA server to discard all packets from the client because it must treat the client as a potential intruder and a threat to the network's security.

Step 6 If you are using NDGs, from the Network Device Group list, select the name of the NDG to which this AAA client should belong, or select **Not Assigned** to set this AAA client to be independent of NDGs.

Note To enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

Step 7 From the Authenticate Using list, select the network security protocol used by the AAA client. Select either one of the following options, or any other custom RADIUS VSA that you have configured:

- **TACACS+ (Cisco IOS)**—Select this option to use TACACS+, which is the standard choice when using Cisco Systems access servers, routers, and firewalls.
- **RADIUS (Cisco Aironet)**—Select this option if the network device is a Cisco Aironet device that supports authentication via Cisco Secure ACS, such as an Access Point 340 or 350. When configured to use the RADIUS (Cisco Aironet) authentication protocol, Cisco Secure ACS first attempts to to authenticate a user by using LEAP; if this fails, Cisco Secure ACS fails over to EAP-TLS.

  Note Aironet authentication is limited to users whose records reside in either the CiscoSecure user database, a Windows NT/2000 user database, or an ODBC user database.

Downloaded from www.Manualslib.com manuals search engine

- **RADIUS (Cisco BBMS)**—Select this option if the network device is a Cisco BBMS network device supporting authentication via RADIUS.
- **RADIUS (IETF)**—Select this option if you are using devices using RADIUS from more than one manufacturer and want to use standard IETF RADIUS attributes. This is also the protocol to select if you want EAP-TLS to be used with Cisco Aironet AAA clients.
- **RADIUS (Cisco IOS/PIX)**—This option enables you to pack commands sent to a Cisco IOS AAA client. The commands are defined in the Group Setup section. Select this option for RADIUS environments in which key TACACS+ functions are required to support Cisco IOS equipment.
- **RADIUS (Cisco VPN 3000)**—Select this option if the network device is a Cisco VPN 3000 series Concentrator.
- **RADIUS (Cisco VPN 5000)**—Select this option if the network device is a Cisco VPN 5000 series Concentrator.
- **RADIUS (Ascend)**—Select this option if the network device is an Ascend network device supporting authentication via RADIUS.
- **RADIUS (Juniper)**—Select this option if the network device is a Juniper network device supporting authentication via RADIUS.
- **RADIUS (Nortel)**—Select this option if the network device is a Nortel network device supporting authentication via RADIUS.

Note The preceding list of protocol options represents those that Cisco Secure ACS ships with. For information about creating user-defined RADIUS VSAs, see the "User-Defined RADIUS Vendors and VSA Sets" section on page E-27.

Step 8 To enable single connection from a AAA client, rather than a new one for every TACACS+ request, select the Single Connect TACACS+ AAA Client (Record stop in accounting on failure) check box. In single connection, multiple requests from a single client are multiplexed over a single session.

Note If your connection is unreliable, do not use this feature.

Downloaded from www.Manualslib.com manuals search engine

Step 9 To enable Watchdog packets, select the **Log Update/Watchdog Packets from this AAA Client** check box. Watchdog packets are interim packets sent periodically during a session. They serve to enable an approximation of session length if the AAA client fails and, thereby, no stop packet is received to mark the end of the session.

Step 10 To allow RADIUS tunneling accounting packets (**tunnel reject/start/stop** and **tunnel link reject/start/stop**) to be logged in the RADIUS Accounting reports of Reports and Activity, select the **Log RADIUS tunneling Packets from this AAA Client** check box.

Step 11 To save your changes and apply them immediately, click **Submit + Restart**.

Note Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter.

Tip To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.

Editing an Existing AAA Client

You can use this procedure to edit the settings for a AAA client.

Note You can not directly edit the name of a AAA client; rather, you must delete the AAA client entry and then re-establish the entry with the corrected name.

To edit a AAA client, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration section opens.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Do one of the following:

a. If you are using NDGs, click the name of the NDG to which the AAA client is assigned. Then, click the name of the AAA client.

b. To edit a AAA client when you have not enabled NDGs, click the name of the AAA client from the AAA Client Hostname column of the AAA Clients table.

Result: The AAA Client Setup For *Name* page appears.

Step 3 In the AAA Client IP Address box, type the corrected IP address assigned to the AAA client, as applicable.

Step 4 In the Key box, type the corrected shared secret, as applicable.

Note For correct operation, the identical key must be configured on the AAA client and Cisco Secure ACS. Keys are case sensitive.

Step 5 If you are using NDGs, from the Network Device Group list, correct the selection of the name of the NDG to which this AAA client should belong, as applicable. To set this AAA client to be independent of NDGs, select **Not Assigned**.

Step 6 From the Authenticate Using list, correct the selection of the network security protocol, as applicable.

Note The previous procedure includes detailed information about these security protocols.

Step 7 Change the status of any of the following three options, as applicable:

- **Single Connect TACACS+ NAS**
- **Log Update/Watchdog Packets from this Access Server**
- **Log RADIUS tunneling Packets from this Access Server**

Downloaded from www.Manualslib.com manuals search engine

Step 8 To save your changes and apply them immediately, click **Submit + Restart**.

Tip To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.

Note Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter.

Deleting a AAA Client

To delete a AAA client, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration section opens.

Step 2 Do one of the following:

a. If you are using NDGs, click the name of the NDG to which the AAA client is assigned. Then, click the AAA client hostname in the AAA Clients table.

b. To delete a AAA client when you have not enabled NDGs, click the AAA client hostname in the AAA Clients table.

Result: The AAA Client Setup for *Name* page appears.

Step 3 To delete the AAA client and have the deletion take effect immediately, click **Delete + Restart**.

Downloaded from www.Manualslib.com manuals search engine

Note Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. As an alternative to restarting when you delete a AAA client, you can click **Delete**. However, when you do this, the change does not take effect until you restart the system, which you can do by clicking **System Configuration**, clicking **Service Control**, and then clicking **Restart**.

Result: A confirmation dialog box appears.

Step 4 Click **OK**.

Result: Cisco Secure ACS performs a restart and the AAA client is deleted.

AAA Server Configuration

This section presents procedures for configuring AAA servers in the Cisco Secure ACS. For additional information about AAA servers, see the AAA Servers in Distributed Systems, page 4-3.

To configure distributed system features for a given Cisco Secure ACS server, you must first define the other AAA server(s).

Tip If the AAA Servers table does not appear, click Interface Configuration, click Advanced Options, and then select the Distributed System Settings check box.

Details on working with AAA servers are given in the following procedures:

- Adding and Configuring a AAA Server, page 4-16
- Editing a AAA Server Configuration, page 4-18
- Deleting a AAA Server, page 4-20

Downloaded from www.Manualslib.com manuals search engine

Adding and Configuring a AAA Server

To add and configure a AAA server, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration section opens.

Step 2 Do one of the following:

a. If you are using NDGs, click the name of the NDG to which the AAA server is to be assigned. Then, click **Add Entry** below the [name] AAA Servers table.

b. To add a AAA server when you have not enabled NDGs, below the AAA Servers table, click **Add Entry**.

Result: The Add AAA Server page appears.

Step 3 If this is a new AAA Server, in the AAA Server Name box, type a name for the remote AAA server.

Step 4 In the AAA Server IP Address box, type the IP address assigned to the remote AAA server.

Step 5 In the Key box, type the shared secret that the remote AAA server and the Cisco Secure ACS use to encrypt the data.

Note The key is case sensitive. If the keys between the two AAA servers are not identical when authentication is forwarded, the request is incorrectly encrypted and authentication fails.

Step 6 From the Network Device Group list, select the NDG to which this AAA Server belongs.

Note To enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then click **Network Device Groups**.

Step 7 To enable Watchdog packets, select the **Log Update/Watchdog Packets from this remote AAA Server** check box. Watchdog packets are interim packets sent periodically during a session. They serve to enable an approximation of session length in the event that no stop packet is received to mark the end of the session.

Downloaded from www.Manualslib.com manuals search engine

Step 8 In the AAA Server Type list, select the protocol the remote AAA server is configured to use:

- **RADIUS**—Select this option if the remote AAA server is configured using any type of RADIUS protocol.
- **TACACS+**—Select this option if the remote AAA server is configured using the TACACS+ protocol.
- **Cisco Secure ACS for Windows 2000/NT**—Select this option if the remote AAA server is another Cisco Secure ACS. This enables you to configure features that are only available with other Cisco Secure ACS servers, such as CiscoSecure user database replication and remote logging.

Note The remote Cisco Secure ACS must be using Version 2.1 or later.

Step 9 The Traffic Type list defines the direction in which traffic to and from the remote AAA server is allowed to flow from this local Cisco Secure ACS. From the Traffic Type list, select one of the following options:

- **Inbound**—The selected AAA server accepts requests that have been forwarded to it and does not forward the request to another AAA server. Select this option if you do not want to allow any authentication requests to be forwarded from the remote AAA server.
- **Outbound**—The selected AAA server sends out authentication requests but does not receive them. If a Proxy Distribution Table entry is configured to proxy authentication requests to a AAA server that is configured for Outbound, the authentication request is not sent.
- **Inbound/Outbound**—The specified AAA server forwards and accepts authentication requests. This allows the selected server to handle authentication requests in any manner defined in the distribution tables.

Downloaded from www.Manualslib.com manuals search engine

Step 10 To save your changes and apply them immediately, click **Submit + Restart**.

Tip To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.

Note Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter and resets it to zero.

Editing a AAA Server Configuration

Use this procedure to edit the settings for a AAA server that you have previously configured.

Note You cannot edit the name of an existing AAA server. To rename a AAA server, you must delete the existing AAA server and then add a new server entry with the new name.

Tip For detailed information on the AAA server settings, see the "Adding and Configuring a AAA Server" section on page 4-16.

Downloaded from www.Manualslib.com manuals search engine

To edit a AAA server configuration, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration section opens.

Step 2 Do one of the following:

a. If you are using NDGs, click the name of the NDG to which the AAA server is assigned. Then, in the AAA Servers table, click the name of the AAA server to be edited.

b. If you have not enabled NDGs, in the AAA Servers table, click the name of the AAA server to be edited.

Result: The AAA Server Setup for *X* page appears.

Step 3 Enter or select new settings for one or more of the following fields:

- AAA Server IP Address
- Key
- Log Update/Watchdog Packets from this remote AAA Server
- AAA Server Type
- Traffic Type

Step 4 To save your changes and apply them immediately, click **Submit + Restart**.

Tip To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.

Note Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter and resets it to zero.

Downloaded from www.Manualslib.com manuals search engine

Deleting a AAA Server

To delete a AAA server, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration section opens.

Step 2 Do one of the following:

a. If you are using NDGs, click the name of the NDG to which the AAA Server is assigned. Then, click the AAA Server Name in the AAA Servers table.

b. If you have not enabled NDGs, click the AAA Server Name in the AAA Servers table.

Result: The AAA Server Setup for *X* page appears.

Step 3 To delete the AAA server and have the deletion take effect immediately, click **Delete + Restart**.

Note Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. As an alternative to restarting when you delete a AAA server, in the preceding step you can click **Delete**. However, when you do this, the change does not take effect until you restart the system, which you can do by clicking **System Configuration**, clicking **Service Control**, and then clicking **Restart**.

Result: A confirmation dialog box appears.

Step 4 Click **OK**.

Result: Cisco Secure ACS performs a restart and the AAA server is deleted.

Network Device Group Configuration

Network Device Grouping is an advanced feature that enables you to view and administer a collection of network devices as a single logical group. To simplify administration, you can assign each group a convenient name that can be used to

Downloaded from www.Manualslib.com manuals search engine

refer to all devices within that group. This creates two levels of network devices within Cisco Secure ACS—single discrete devices such as an individual router or network access server, and an NDG; that is, a collection of routers or AAA servers.

This section contains the following procedures for working with NDGs:

- Adding a Network Device Group, page 4-21
- Assigning an Unassigned AAA Client or AAA Server to an NDG, page 4-22
- Reassigning a AAA Client or AAA Server to an NDG, page 4-23
- Renaming a Network Device Group, page 4-23
- Deleting a Network Device Group, page 4-24

Adding a Network Device Group

You can assign users or groups of users to NDGs. For more information, see one of the following:

- Setting TACACS+ Enable Password Options for a User, page 7-34
- Setting Enable Privilege Options for a User Group, page 6-18

To add an NDG, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration section opens.

Step 2 Beneath the Network Device Groups table, click **Add Entry**.

Tip If the Network Device Groups table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select **Network Device Groups**.

Step 3 In the Network Device Group Name box, type the name of the new NDG.

Tip The maximum name length is 19 characters. Quotation marks (") and commas (,) are not allowed. Spaces are allowed.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Click **Submit**.

Result: The Network Device Groups table displays the new NDG.

Step 5 To populate the newly established NDG with AAA clients or AAA servers, perform one or more of the following procedures, as applicable:

- Adding and Configuring a AAA Client, page 4-9
- Assigning an Unassigned AAA Client or AAA Server to an NDG, page 4-22
- Reassigning a AAA Client or AAA Server to an NDG, page 4-23
- Adding and Configuring a AAA Server, page 4-16

Assigning an Unassigned AAA Client or AAA Server to an NDG

You use this procedure to assign an unassigned AAA client or AAA server to an NDG. A prerequisite to performing this procedure is that you have already configured the client or server and it appears in the Not Assigned AAA Clients or Not Assigned AAA Servers table.

To assign a network device to an NDG, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration section opens.

Step 2 In the Network Device Groups table, click **Not Assigned**.

Tip If the Network Device Groups table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

Step 3 Click the name of the network device you want to assign to an NDG.

Downloaded from www.Manualslib.com manuals search engine

Step 4 From the Network Device Groups list, select the NDG to which you want to assign the AAA client or AAA server.

Step 5 Click **Submit**.

Result: The client or server is assigned to an NDG.

Reassigning a AAA Client or AAA Server to an NDG

To reassign a AAA client or AAA server to a new NDG, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration section opens.

Step 2 In the Network Device Groups table, click the name of the network device's current group.

Step 3 In either the AAA Clients table or AAA Servers table, as applicable, click the name of the client or server you want to assign to a new NDG.

Step 4 From the Network Device Group list, select the NDG to which you want to reassign the network device.

Step 5 Click **Submit**.

Result: The network device is assigned to a different NDG.

Renaming a Network Device Group

To rename an NDG, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration section opens.

Step 2 In the Network Device Groups table, click the NDG to be renamed.

Downloaded from www.Manualslib.com manuals search engine

Tip If the Network Device Groups table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

Step 3 At the bottom of the page, click **Rename**.

Result: The Rename Network Device Group page appears.

Step 4 In the Network Device Group Name box, type the new name.

Step 5 Click **Submit**.

Result: The name of the NDG is changed.

Deleting a Network Device Group

To delete an NDG, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration section opens.

Step 2 In the Network Device Groups table, click the NDG to be deleted.

Tip If the Network Device Groups table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

Step 3 At the bottom of the page, click **Delete Group**.

Result: A confirmation dialog box appears.

Step 4 Click **OK**.

Result: The name of the NDG is changed.

Downloaded from www.Manualslib.com manuals search engine

Proxy Distribution Table Configuration

This section begins with a description of the Proxy Distribution Table and then details the following Proxy Distribution Table configuration procedures:

- Adding a New Proxy Distribution Table Entry, page 4-26
- Sorting the Character String Match Order of Distribution Entries, page 4-28
- Editing a Proxy Distribution Table Entry, page 4-28
- Deleting a Proxy Distribution Table Entry, page 4-29

About the Proxy Distribution Table

If you have Distributed Systems Settings enabled, when you click **Network Configuration**, you will see the Proxy Distribution Table.

Tip To enable Distributed Systems Settings in the Cisco Secure ACS, click **Interface Configuration**, click **Advanced Options**, and then select the **Distributed System Settings** check box.

The Proxy Distribution Table comprises entries that show the character strings on which to proxy, the AAA Servers to proxy to, whether to strip the character string, and where to send the accounting information (Local/Remote, Remote, or Local). For more information about the proxy feature, see the "Proxy in Distributed Systems" section on page 4-4.

The entries you define and place in the Proxy Distribution Table can be considered turnstiles for each authentication request that Cisco Secure ACS receives from the AAA client. How the authentication request is defined in the Proxy Distribution Table depends on where it is to be forwarded. If a match to an entry in the Proxy Distribution Table that contains proxy information is found, Cisco Secure ACS forwards the request to the appropriate AAA server.

The Character String column in the Proxy Distribution Table always contains an entry of "(Default)". The "(Default)" entry matches authentication requests received by the local Cisco Secure ACS server that do not match any other defined character strings. While you cannot change the character string definition for the "(Default)" entry, you can change the distribution of authentication requests matching the "(Default)" entry. At installation, the AAA server associated with

Downloaded from www.Manualslib.com manuals search engine

the "(Default)" entry is the local Cisco Secure ACS server. It can sometimes be easier to define strings that match authentication requests to be processed locally rather than defining strings that match authentication requests to be processed remotely. In such a case, associating the "(Default)" entry with a remote AAA server permits you to configure your Proxy Distribution Table with the more easily written entries.

Adding a New Proxy Distribution Table Entry

To create a Proxy Distribution Table entry, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration page opens.

Step 2 Below the Proxy Distribution Table, click **Add Entry**.

Note If the Proxy Distribution Table does not appear, you must enable it by clicking Interface Configuration, clicking **Advanced Options**, and then selecting the **Distributed System Settings** check box.

Step 3 In the Character String box, type the string of characters, including the delimiter to forward on when users dial in to be authenticated. For example,.uk.

Note Angle brackets (< and >) cannot be used.

Step 4 From the Position list, select **Prefix** if the character string you typed appears at the beginning of the username or **Suffix** if the character string appears at the end of the username.

Step 5 From the Strip list, select **Yes** if the character string you entered is to be stripped off the username, or select **No** if it is to be left intact.

Step 6 In the AAA Servers column, select the AAA server you want to use for proxy. Click —> (right arrow button) to move it to the Forward To column.

Downloaded from www.Manualslib.com manuals search engine

Tip You can also select additional AAA servers to use for backup proxy in the event the prior servers fail. To set the order of AAA servers, in the Forward To column, click the name of the applicable server and click **Up** or **Down** to move it into the position you want.

Tip If the AAA server you want to use is not listed, click **Network Configuration**, click **AAA Servers**, click **Add Entry** and complete the applicable information.

Step 7 From the Send Accounting Information list, select one of the following areas to which to report accounting information:

- **Local**—Keep accounting packets on the local Cisco Secure ACS.
- **Remote**—Send accounting packets to the remote Cisco Secure ACS.
- **Local/Remote**—Keep accounting packets on the local Cisco Secure ACS and send them to the remote Cisco Secure ACS.

Tip This information is especially important if you are using the Max Sessions feature to control the number of connections a user is allowed. Max Sessions depends on accounting start and stop records, and where the accounting information is sent determines where the Max Sessions counter is tracked. The Failed Attempts log and the Logged in Users report are also affected by where the accounting records are sent.

Step 8 When you have finished, click **Submit** or **Submit + Restart**.

Downloaded from www.Manualslib.com manuals search engine

Sorting the Character String Match Order of Distribution Entries

You can use this procedure to set the priority by which Cisco Secure ACS searches character string entries in the Proxy Distribution Table when users dial in.

To determine the priority order by which Cisco Secure ACS searches entries in the Proxy Distribution Table, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration page opens.

Step 2 Below the Proxy Distribution Table, click **Sort Entries**.

Tip To be able to sort the entries, you must have already configured at least two unique Proxy Distribution Table entries in addition to the default table entry.

Step 3 Select the character string entry to reorder, and then click **Up** or **Down** to move its position to reflect the search order you want.

Step 4 When you have finished sorting, click **Submit** or **Submit + Restart**.

Editing a Proxy Distribution Table Entry

To edit a Proxy Distribution Table entry, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration page opens.

Step 2 In the Character String column of the Proxy Distribution Table, click the distribution entry you want to edit.

Result: The Edit Proxy Distribution Entry page appears.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Edit the entry as necessary.

Tip For information about the parameters that make up a distribution entry, see the "Adding a New Proxy Distribution Table Entry" section on page 4-26.

Step 4 When you have finished editing the entry, click **Submit** or **Submit + Restart**.

Deleting a Proxy Distribution Table Entry

To delete a Proxy Distribution Table entry, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

Result: The Network Configuration page opens.

Step 2 In the Character String column of the Proxy Distribution Table, click the distribution entry you want to delete.

Result: The Edit Proxy Distribution Entry page appears.

Step 3 Click **Delete**.

Result: A confirmation dialog box appears.

Step 4 Click **OK**.

Result: Cisco Secure ACS deletes the distribution entry from the Proxy Distribution Table.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 5

Setting Up and Managing Shared Profile Components

The Shared Profile Components section enables administrators to develop and name reusable, shared sets of authorization components which may be applied to one or more users or groups of users and referenced by name within their profiles. These comprise network access restrictions (NARs), command authorization sets, and downloadable PIX ACLs.

The Shared Profile Components section of Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) addresses the scalability of selective authorization. Shared profile components can be configured once and then applied to many users or groups. Without this ability, flexible and comprehensive authorization could only be accomplished by explicitly configuring the authorization of each user group for each possible command on each possible device. The creation and application of these named shared profile components (access restrictions, command sets, and ACLs) make it unnecessary to repeatedly enter long lists of devices or commands when defining network access parameters.

Shared profile components also provide the means for one device to issue a command on behalf of another device or devices. Their scalability extends to the following capabilities:

- A means to determine the list of commands a user could issue against one or more devices in the network
- A means to determine the list of devices on which a particular user may execute a particular command.

Downloaded from www.Manualslib.com manuals search engine

This chapter contains the following sections:

- Downloadable PIX ACLs, page 5-2
- Network Access Restrictions, page 5-6
- Command Authorization Sets, page 5-12

Downloadable PIX ACLs

This section includes a description of downloadable PIX ACLs followed by detailed instructions regarding their configuration and management.

About Downloadable PIX ACLs

Downloadable PIX ACLs enable you to enter an ACL once, in Cisco Secure ACS, and then load that ACL to any number of PIX Firewalls that authenticate using the Cisco IOS/PIX protocol. This is far more efficient than directly entering the ACL into each PIX Firewall via its CLI. No additional configuration of the PIX Firewall is necessary after it has been configured to undertake authorization using RADIUS.

The ACL Definitions that you enter into Cisco Secure ACS consist of one or more PIX ACL commands, with each command on a separate line. Using standard RADIUS Cisco AV-pairs permits you to enter a maximum of 4 kilobytes of ACLs; whereas, the downloadable PIX ACLs can be of unlimited size. In entering the ACL definitions in the ACS HTML interface, do not use keyword and name entries; in all other respects, use standard PIX ACL command syntax and semantics. An example of the format you should use to enter ACL Definitions follows:

```
permit tcp any host 11.0.0.254

permit udp any host 11.0.0.254

permit icmp any host 11.0.0.254

permit tcp any host 11.0.0.253
```

See the “Command Reference” section of your PIX Firewall configuration guide for detailed ACL definition information.

Downloaded from www.Manualslib.com manuals search engine

ACLs entered into the Cisco Secure ACS are protected by whatever backup or replication regime you have established for the Cisco Secure ACS. After you configure an ACL as a named shared profile component, you can include that ACL in any Cisco Secure ACS user, or user group, profile. When Cisco Secure ACS returns an attribute with a named ACL as part of a user's session RADIUS access accept packet, the PIX Firewall applies that ACL to that user's session. Cisco Secure ACS employs a versioning stamp for ensuring that the PIX Firewall has cached the latest ACL version. If a PIX Firewall responds that it does not have the current version of the named ACL in its cache (that is, the ACL is new or has changed), Cisco Secure ACS automatically uploads the ACL update to the PIX Firewall cache.

After you configure a downloadable PIX ACL, it can be applied against any number of single users or user groups.

Downloadable PIX ACL Configuration

This section contains the following procedures:

- Adding a Downloadable PIX ACL, page 5-3
- Editing a Downloadable PIX ACL, page 5-4
- Deleting a Downloadable PIX ACL, page 5-5

Adding a Downloadable PIX ACL

To add a downloadable PIX ACL, follow these steps:

Step 1 In the navigation bar, click **Shared Profile Components**.

Result: The Shared Profile Components page appears.

Step 2 Click **Downloadable PIX ACLs**.

Step 3 Click **Add**.

Result: The Downloadable PIX ACLs page appears.

Step 4 In the **Name:** box, type the name of the new PIX ACL.

Downloaded from www.Manualslib.com manuals search engine

Note The name of a PIX ACL may contain up to 32 characters. The name *may* contain spaces; but it *may not* contain leading, trailing, or multiple spaces, or the following characters: - [ ] / —

Step 5 In the **Description:** box, type a description of the new PIX ACL.

Step 6 In the **ACL Definitions** box, type the new PIX ACL definitions.

Note In entering the ACL definitions in the ACS HTML interface, you do not use keyword and name entries; rather, you begin with a permit/deny keyword. For an example of the proper format of the ACL definitions, see the "About Downloadable PIX ACLs" section on page 5-2.

Step 7 When you have completed specifying the PIX ACL, click **Submit**.

Result: Cisco Secure ACS enters the new PIX ACL, which takes effect immediately. That is, it is available to be sent to any PIX Firewall that is attempting authentication of a user who has that ACL name as part of his or her user or group profile. For information on assigning a user or a group to a PIX ACL, see the "Assigning a PIX ACL to a User" section on page 7-22 or the "Assigning a Downloadable PIX ACL to a Group" section on page 6-27, respectively.

Editing a Downloadable PIX ACL

To edit a downloadable PIX ACL, follow these steps:

Step 1 In the navigation bar, click **Shared Profile Components**.

Result: The Shared Profile Components page appears.

Step 2 Click **Downloadable PIX ACLs**.

Result: The Downloadable PIX ACLs table appears.

Downloaded from www.Manualslib.com manuals search engine

Step 3 In the Name column, click the PIX ACL you want to edit.

Result: The Downloadable PIX ACLs page appears with information displayed for the selected filter.

Step 4 Edit the **Name** or **Description** or **ACL Definitions** information, as applicable.

Step 5 When you have finished editing the information for the PIX ACL, click **Submit**.

Result: Cisco Secure ACS re-enters the PIX ACL with the new information, which takes effect immediately.

Deleting a Downloadable PIX ACL

Before You Begin

You should remove a PIX ACL's association with any user, or user group, profile before deleting it.

To delete a PIX ACL, follow these steps:

Step 1 In the navigation bar, click **Shared Profile Components**.

Result: The Shared Profile Components page appears.

Step 2 Click **Downloadable PIX ACLs**.

Step 3 Click the name of the downloadable PIX ACL you want to edit.

Result: The Downloadable PIX ACLs page appears with information displayed for the selected PIX ACL.

Step 4 At the bottom of the page, click **Delete**.

Result: A dialog box warns you that you are about to delete a PIX ACL.

Step 5 To confirm that you intend to delete the PIX ACL, click **OK**.

Result: The selected PIX ACL is deleted.

Downloaded from www.Manualslib.com manuals search engine

Network Access Restrictions

This section includes a description of NARs followed by detailed instructions regarding shared NAR access configuration and management.

About Network Access Restrictions

NARs enable you to define additional authorization conditions that must be met before a user can gain access to the network. Cisco Secure ACS supports two basic types of network access restrictions:

- IP-based restrictions where the originating request relates to an existing IP address
- Non-IP-based filters for all other cases where automatic number identification (ANI) may be used

A non-IP-based NAR is a list of permitted or denied “calling”/“point of access” locations that you can employ in restricting a AAA client when you do not have an IP-based connection established. The non-IP-based NAR generally uses the calling line ID (CLI) number and the Dialed Number Identification Service (DNIS) number.

However, you can use the non-IP-based filter even when the AAA client does not use a Cisco IOS release that supports CLI or DNIS by entering a IP address in place of the CLI. In another exception to entering a CLI, you can enter a MAC address to permit or deny; for example when you are using a Cisco Aironet AAA client. Likewise, you could enter a the Cisco Aironet AP MAC address in place of the DNIS. The format of what you specify in the CLI box—be it CLI, IP address, or MAC address—must match the format of what you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

When specifying a NAR you may use asterisks (*) as wildcards for any value, or as part of any value to establish a range. Cisco Secure ACS also accepts comma separated values in NAR definitions. All the values/conditions in a NAR specification must be met for the NAR to restrict access; that is, the values are “ANDed”.

Downloaded from www.Manualslib.com manuals search engine

Note When an authentication request is forwarded by proxy to a Cisco Secure ACS, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

You can define a NAR for, and apply it to, a single, particular user or user group. For more information on this, see the "Setting Network Access Restrictions for a User" section on page 7-12 or the "Setting Network Access Restrictions for a User Group" section on page 6-7. However, in the Shared Profile Components section of Cisco Secure ACS you can create and name a shared NAR without directly citing any user or user group. You give the shared NAR a name that can be referenced in other parts of the Cisco Secure ACS HTML interface. Then, when you set up users or user groups, you can select none, one, or multiple shared restrictions to be applied. When you specify the application of multiple shared NARs to a user or user group, you choose one of two access criteria: either "All selected filters must permit", or "Any one selected filter must permit".

Shared access restrictions are kept in the CiscoSecure user database and can be backed up/restored by the Cisco Secure ACS backup and restore features and replicated to secondary Cisco Secure ACS servers along with other configurations.

Shared Network Access Restrictions Configuration

You can configure multiple shared NARs to restrict access to particular AAA clients, all AAA clients, or to named NDGs.

This section contains the following procedures:

- Adding a Shared Network Access Restriction, page 5-8
- Editing a Shared Network Access Restriction, page 5-10
- Deleting a Shared Network Access Restriction, page 5-12

Downloaded from www.Manualslib.com manuals search engine

Adding a Shared Network Access Restriction

To add a shared NAR, follow these steps:

Step 1 In the navigation bar, click **Shared Profile Components**.

Result: The Shared Profile Components page appears.

Step 2 Click **Network Access Restrictions**.

Step 3 Click **Add**.

Result: The Network Access Restriction page appears.

Step 4 In the Name box, type a name for the new shared NAR.

Note The name can contain up to 32 characters. Leading and trailing spaces are not allowed. Names cannot contain the following four special characters: [ ] , /

Step 5 In the Description box, type a description of the new shared NAR.

Step 6 To permit or deny access based on IP addressing, follow these steps:

Note This step is performed for IP-based restrictions where an IP connection exists. For other restriction types, see the "About Network Access Restrictions" section on page 5-6.

a. Select the **Define IP-based access descriptions** check box.

b. To specify whether you are listing addresses that are permitted or denied, from the Table Defines list, select the applicable value.

Downloaded from www.Manualslib.com manuals search engine

c. Select or type the applicable information in each of the following boxes:

- **AAA Client**—Select **All AAA clients**, or the name of the network device group (NDG), or the individual AAA client, to which access is permitted or denied.
- **Port**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports on the selected AAA client.
- **Src IP Address**—Type the IP address to filter on when performing access restrictions. You can type multiple entries separated by a comma or use the wildcard asterisk (*) to specify all IP addresses.

d. Click **enter**.

Result: The AAA client, port, and address information appears as a line item in the table.

e. To enter additional IP-based line items, repeat Steps c and d.

Step 7 To permit or deny access based on calling location or values other than an established IP address, follow these steps:

a. Select the **Define CLI/DNIS based access restrictions** check box.

b. To specify whether you are listing addresses that are permitted or denied, from the Table Defines list, select the applicable value.

c. To specify the applicability of this NAR, from the AAA Client list, select one of the following values:

- The name of the NDG
- The name of the particular AAA client
- All AAA clients

Tip Only NDGs that you have previously configured appear in the list.

Downloaded from www.Manualslib.com manuals search engine

d. To specify the information that this NAR should filter on, fill in the following boxes, as applicable:

Tip You can type an asterisk (*) as a wild card to specify "all" either as a value or within a range.

- **Port**—Type the number of the port to filter on.
- **CLI**—Type the CLI number to filter on. You can also use this box to restrict access based on values other than CLIs, such as an IP address or MAC address; for information, see the "About Network Access Restrictions" section on page 5-6.
- **DNIS**—Type the number being dialed into to filter on.

e. Click **enter**.

Result: The information specifying the NAR line item appears in the table.

f. To enter additional non-IP based NAR line items, repeat Steps C through E.

Step 8 When you are finished defining the shared NAR, click **Submit**.

Result: Cisco Secure ACS saves the named shared NAR and lists it in the Network Access Restriction Sets table.

Editing a Shared Network Access Restriction

To edit a shared network access restriction, follow these steps:

Step 1 In the navigation bar, click **Shared Profile Components**.

Result: The Shared Profile Components page appears.

Step 2 Click **Network Access Restrictions**.

Result: The Network Access Restrictions table appears.

Step 3 In the Name column, click the shared NAR you want to edit.

Result: The Network Access Restriction page appears with information displayed for the selected filter.

Downloaded from www.Manualslib.com manuals search engine

Step 4 To edit the Name or Description of the filter, type and delete information, as applicable.

Step 5 To edit a line item in the IP-based access restrictions table, follow these steps:

a. Double-click the line item to be edited.

Result: Information for the line item is removed from the table and written to the boxes below the table.

b. Edit the information, as applicable.

c. Click **enter**.

Result: The edited information for this line item is written to the IP-based access restrictions table.

Step 6 To remove a line item from the IP-based access restrictions table, follow these steps:

a. Select the line item.

b. Below the table, click **remove**.

Result: The line item is removed from the IP-based access restrictions table.

Step 7 To edit a line item in the CLI/DNIS access restrictions table, follow these steps:

a. Double-click the line item to be edited.

Result: Information for the line item is removed from the table and written to the boxes below the table.

b. Edit the information, as applicable.

c. Click **enter**.

Result: The edited information for this line item is written to the CLI/DNIS access restrictions table.

Step 8 To remove a line item from the CLI/DNIS access restrictions table, follow these steps:

a. Select the line item.

b. Below the table, click **remove**.

Result: The line item is removed from the CLI/DNIS access restrictions table.

Downloaded from www.Manualslib.com manuals search engine

Step 9 When you have finished editing the line items that make up the filter, click **Submit**.

Result: Cisco Secure ACS re-enters the filter with the new information, which takes effect immediately.

Deleting a Shared Network Access Restriction

To delete a shared network access restriction, follow these steps:

Step 1 In the navigation bar, click **Shared Profile Components**.

Result: The Shared Profile Components page appears.

Step 2 Click **Network Access Restrictions**.

Step 3 Click the Name of the shared NAR you want to delete.

Result: The Network Access Restriction page appears with information displayed for the selected NAR.

Step 4 At the bottom of the page, click **Delete**.

Result: A dialog box warns you that you are about to delete a shared NAR.

Step 5 To confirm that you intend to delete the shared NAR, click **OK**.

Result: The selected shared NAR is deleted.

Command Authorization Sets

This section includes a description of command authorization sets and pattern matching followed by detailed instructions regarding their configuration and management.

Downloaded from www.Manualslib.com manuals search engine

About Command Authorization Sets

Command authorization sets provide a central mechanism to control the authorization of each command on each network device. This greatly enhances the scalability and manageability of setting authorization restrictions. In Cisco Secure ACS, the default command authorization sets include the Shell Command Authorization Sets and the PIX Command Authorization Sets. Other Cisco network management applications, such as CiscoWorks2000, may be enabled to instruct ACS to support additional command authorization set types.

To offer fine-grained control of network devices, by administrators, using a Telnet administration session, a network device using TACACS+ can request authorization for each command line before its execution. Cisco Secure ACS administrators can define a set of commands, which are either permitted or denied for execution by a particular user on a given device. Cisco Secure ACS has further enhanced this capability as follows:

- **Reusable Named Command Authorization Sets**—You can create a named set of device commands without directly citing any user or user group. The administrator can define a number of device command sets, each of which delineates different access profiles. For example, a “help desk” device command set could permit access to high level browsing commands, such as “show run”, and deny any configuration commands. An “All network engineers” command set could contain a limited list of permitted device commands for any network engineer in the enterprise. The “Local Network Engineers” command set could permit all device commands, including IP-address configuration.
- **Finer Configuration Granularity**—You can create associations between named command authorization sets and NDGs. Thus, you are able to define different access profiles for users depending on which network devices they access. You can associate the same named command authorization set with more than one NDG and use it for more than one user group.
  Cisco Secure ACS enforces data integrity. Named command authorization sets are kept in the CiscoSecure user database and can be backed up/restored by the Cisco Secure ACS backup and restore features and replicated to secondary Cisco Secure ACS servers along with other configuration.

Downloaded from www.Manualslib.com manuals search engine

For information on assigning command authorization sets, see the following procedures:

- **Shell Command Authorization Sets**—See either of the following:
  - Configuring a Shell Command Authorization Set for a User Group, page 6-30
  - Configuring a Shell Command Authorization Set for a User, page 7-26
- **PIX Command Authorization Sets**—See either of the following:
  - Configuring a PIX Command Authorization Set for a User Group, page 6-32
  - Configuring a PIX Command Authorization Set for a User, page 7-29

About Pattern Matching

For permit/deny command arguments, Cisco Secure ACS applies pattern matching. That is, the argument **permit foo** matches any argument that contains the string **foo**. Thus, for example, **permit foo** would allow not only the argument **foo** but also the arguments **anyfoo** and **foobar**.

To limit the extent of pattern matching you can add the following expressions:

- **dollarsign ($)**—Expresses that the argument must end with what has gone before. Thus **permit foo$** would match against **foo** or **anyfoo**, but not **foobar**.
- **caret (^)**—Expresses that the argument must begin with what follows. Thus **permit ^foo** would match against **foo** or **foobar**, but not against **anyfoo**.

You can combine these expressions to specify absolute matching. In the example given, you would use **permit ^foo$** to ensure that only **foo** was permitted, and not **anyfoo** or **foobar**.

Command Authorization Sets Configuration

This section contains the following procedures:

- Adding a Command Authorization Set, page 5-15
- Editing a Command Authorization Set, page 5-17
- Deleting a Command Authorization Set, page 5-17

Downloaded from www.Manualslib.com manuals search engine

Adding a Command Authorization Set

To add a command authorization set, follow these steps:

Step 1 In the navigation bar, click **Shared Profile Components**.

Result: The Shared Profile Components page lists the command authorization set types available. These always include Shell Command Authorization Sets and PIX Command Authorization Sets.

Step 2 Click one of the listed command authorization set types, as applicable.

Result: The selected Command Authorization Sets table appears.

Step 3 Click **Add**.

Result: The applicable Command Authorization Set page appears.

Step 4 In the Name box, type a name for the command authorization set

Note The set name can contain up to 32 characters. Names cannot contain the following special characters:
? " * > <
Leading and trailing spaces are not allowed.

Step 5 In the Description box, type a description of the command authorization set.

Step 6 To specify how Cisco Secure ACS is to handle unmatched commands, select either the **Permit** or **Deny** option, as applicable.

Tip The default setting is Deny.

Downloaded from www.Manualslib.com manuals search engine

Step 7 For each command you want to enter as part of this command authorization set, follow these steps:

a. In the box just above the Add Command button, type a command that is to be part of the set.

Note Enter only the command portion of the command/argument string here. Arguments are added only after the command is listed. For example, with the command/argument string "show run" you would type only the command **show**.

b. Click **Add Command**.

Result: The typed command is added to the command list box.

c. To add an argument to a command, in the command list box, select the command and then type the argument in the box to the right of the command.

Note The correct format for arguments is <permit | deny> <argument>. For example, with the command **show** already listed, you might enter **permit run** as the argument.

Tip You can list several arguments for a single command by pressing Enter between arguments.

d. To allow arguments, which you have not listed, to be effective with this command, select the **Permit Unmatched Args** check box.

Step 8 When you are finished adding commands and associated arguments, click **Submit**.

Result: Cisco Secure ACS displays the name and description of the new command authorization set in the applicable Command Authorization Sets table.

Downloaded from www.Manualslib.com manuals search engine

Editing a Command Authorization Set

To edit a command authorization set, follow these steps:

Step 1 In the navigation bar, click **Shared Profile Components**.

Result: The Shared Profile Components page lists the command authorization set types available.

Step 2 Click a command authorization set, as applicable.

Result: The selected Command Authorization Sets table appears.

Step 3 From the Name column, click the name of the set you want to change.

Result: Information for the selected set appears on the applicable Command Authorization Set page.

Step 4 Do any or all of the following:

a. To change the set's Name or Description, edit the words in the corresponding box.

b. To remove a command from the set, from the Matched Commands list, select the command, and then click **Remove Command**.

c. To edit a command's arguments, from the command list box, select the command and then type changes to the arguments in the box to the right of the command list box.

Step 5 When you have finished editing the set, click **Submit**.

Deleting a Command Authorization Set

To delete a command authorization set, follow these steps:

Step 1 In the navigation bar, click **Shared Profile Components**.

Result: The Shared Profile Components page lists the command authorization set types available.

Step 2 Click a command authorization set, as applicable.

Result: The selected Command Authorization Sets table appears.

Downloaded from www.Manualslib.com manuals search engine

Step 3 From the Name column, click the name of the command set you want to delete.

Result: Information for the selected set appears on the applicable Command Authorization Set page.

Step 4 Click **Delete**.

Result: A dialog box warns you that you are about to delete an command authorization set.

Step 5 To confirm that you intend to delete that command authorization set, click **OK**.

Result: Cisco Secure ACS displays the applicable Command Authorization Sets table. The command authorization set no longer listed.

Downloaded from www.Manualslib.com manuals search engine

Setting Up and Managing User Groups

This chapter provides information about setting up and managing user groups in the Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) to control authorization. Cisco Secure ACS enables you to group together network users for more efficient administration. You can establish up to 500 different groups to effect different levels of authorization. Cisco Secure ACS also supports external database group mapping; that is, if your external user database distinguishes user groups, these groups can be mapped into Cisco Secure ACS. And if the external database does not support groups, you can map all users from that database to a Cisco Secure ACS user group. For information about external database mapping, see the "Database Group Mappings" section on page 12-10.

Before you configure Group Setup, it is important to understand how this section functions. Cisco Secure ACS dynamically builds the Group Setup section interface depending on the configuration of your network devices and the security protocols being used. That is, what you see under Group Setup is affected by two factors:

- Your system configuration
- Your settings in the Interface Configuration section

This chapter contains the following sections:

- **User Group Setup Features and Functions, page 6-2**—This section is an overview of the features you find within Group Setup.
- **Common User Group Settings, page 6-3**—This section details procedures that you typically would perform regardless of your particular network security configuration.

Downloaded from www.Manualslib.com manuals search engine

- **Configuration-specific User Group Settings, page 6-15**—This section details procedures that you would perform only as applicable to your particular network security configuration.
- **Group Setting Management, page 6-48**—This section includes basic administrative procedures, such as determining the users in a group or renaming a group.

User Group Setup Features and Functions

The Group Setup section of the Cisco Secure ACS HTML interface is the centralized location for operations regarding user group configuration and administration. For information about network device groups (NDGs), see the "Network Device Group Configuration" section on page 4-20.

Default Group

If you have not configured group mapping for an external user database, Cisco Secure ACS assigns users who are authenticated by the Unknown User Policy to the Default Group the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, Cisco Secure ACS retains the group mappings you configured before upgrading.

Group TACACS+ Settings

Cisco Secure ACS enables a full range of settings for TACACS+ at the group level. If a AAA client has been configured to use TACACS+ as the security control protocol, you can configure standard service protocols, including PPP IP, PPP LCP, ARAP, SLIP, and Shell(exec), to be applied for the authorization of each user who belongs to a particular group.

Note You can also configure TACACS+ settings at the individual user level. User-level settings always override group level settings.

Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS also enables you to enter and configure new TACACS+ services. For information about how to configure a new TACACS+ service to appear on the group setup page, see the "Protocol Configuration Options for TACACS+" section on page 3-7.

You can use the Shell Command Authorization Set feature to configure TACACS+ group settings. This feature enables you to apply shell commands to a particular user group in the following ways:

- Assign a shell command authorization set, which you have previously configured, for any network device.
- Assign a shell command authorization set, which you have previously configured, to particular NDGs.
- Permit or deny specific shell commands, which you define, on a per-group basis.

For more information about shell command authorization sets, see Chapter 5, "Setting Up and Managing Shared Profile Components."

Common User Group Settings

This section presents the basic activities you perform when configuring a new user group. This section contains the following procedures:

- Enabling VoIP Support for a User Group, page 6-4
- Setting Default Time of Day Access for a User Group, page 6-5
- Setting Callback Options for a User Group, page 6-6
- Setting Network Access Restrictions for a User Group, page 6-7
- Setting Max Sessions for a User Group, page 6-11
- Setting Usage Quotas for a User Group, page 6-13

Downloaded from www.Manualslib.com manuals search engine

Enabling VoIP Support for a User Group

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Voice-over-IP (VoIP) Group Settings** check box.

Perform this procedure to enable support for the null password function of VoIP. This enables users to authenticate (session or telephone call) on only the user ID (telephone number).

When you enable VoIP at the group level, all users in this group become VoIP users, and the user IDs are treated similarly to a telephone number. VoIP users do not need to enter passwords to authenticate.

Caution Enabling VoIP disables password authentication and most advanced settings, including password aging and protocol attributes.

To enable VoIP support for a group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select the group you want to configure for VoIP support, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 In the Voice-over-IP Support table, select the check box labeled **This is a Voice-over-IP (VoIP) group - and all users of this group are VoIP users**.

Step 4 To save the group settings you have just made, click **Submit**.
For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 5 To continue, and specify other group settings, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Setting Default Time of Day Access for a User Group

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**. Then select the **Default Time-of-Day / Day-of-Week Specification** check box.

To define the times during which users in a particular group are allowed, or not allowed access, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 In the Default Time-of-Day Access Settings table, select the **Set as default Access Times** check box.

Note You must select the **Set as default Access Times** check box, to limit access based on time or day.

Result: Times at which the system allows access are highlighted in green on the day and hour matrix.

Note The default sets accessibility during all hours.

Step 4 In the day and hour matrix, click the times at which you do *not* want to allow access to members of this group.

Tip Clicking times of day on the graph deselects those times; clicking again reselects them.
At any time, you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

Downloaded from www.Manualslib.com manuals search engine

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Callback Options for a User Group

Callback is a command string that is passed back to the access server. You can use callback strings to initiate a modem to call the user back on a specific number for added security or reversal of line charges. There are three options, as follows:

- **No callback allowed**—Disables callback for this group's users. This is the default setting.
- **Dialup client specifies callback number**—Allows the dialup client to specify the callback number. The dialup client must support RFC 1570, PPP LCP Extensions.
- **Use Microsoft NT/2000 Callback settings (where possible)**—Uses the Microsoft Windows NT/2000 callback settings. Note that, if a user's Windows account resides in a remote domain, the domain in which Cisco Secure ACS resides must have a two-way trust with that domain for the Microsoft NT/2000 callback settings to operate for that user.

To set callback options for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 Select a group from the Group list, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 In the Callback table, select one of the following three options:

- No callback allowed
- Dialup client specifies callback number
- Use Microsoft NT/2000 Callback settings (where possible)

Downloaded from www.Manualslib.com manuals search engine

Step 4 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 5 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Network Access Restrictions for a User Group

The Network Access Restrictions table in the Advanced Settings area of Group Setup enables you to apply network access restrictions (NARs) in three distinct ways:

- Apply existing shared NARs by name
- Define IP-based group access restrictions to permit or deny access to a specified AAA client or to specified ports on a AAA client when an IP connection has been established
- Define CLI/DNIS-based group NARs to permit or deny access to either, or both, the calling line ID (CLI) number or the Dialed Number Identification Service (DNIS) number used

Note You can also use the CLI/DNIS-based access restrictions area to specify other values. For more information, see the "About Network Access Restrictions" section on page 5-6.

Typically, you define (shared) NARs from within the Shared Components section so that these restrictions can be applied to more than one group or user. For more information, see the "Shared Network Access Restrictions Configuration" section on page 5-7. You must have enabled the Group-Level Shared Network Access Restriction check box on the Advanced Options page of the Interface Configuration section for this set of options to appear in the Cisco Secure ACS HTML interface.

However, Cisco Secure ACS also enables you to define and apply a NAR for a single group from within the Group Setup section. You must have enabled the Group-Level Network Access Restriction setting under the Advanced Options

Downloaded from www.Manualslib.com manuals search engine

page of the Interface Configuration section for single group IP-based filter options and single group CLI/DNIS-based filter options to appear in the Cisco Secure ACS HTML interface.

Note When an authentication request is forwarded by proxy to a Cisco Secure ACS server, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

To set NARs for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 To apply a previously configured shared NAR to this group, follow these steps:

Note To apply a shared NAR, you must previously have configured it under Network Access Restrictions in the Shared Profile Components section. For more information, see the "Shared Network Access Restrictions Configuration" section on page 5-7.

a. Select the check box labeled **Only Allow network access when**.

b. To specify whether one or all shared NARs must apply for a member of the group to be permitted access, select one of the following two options:

- **All selected shared NARS result in permit**
- **Any one selected shared NAR results in permit**

c. Select a shared NAR name in the Shared NAR list and then click —> (right arrow button) to move the name into the Selected Shared NARs list.

Tip To view the server details of the shared NARs you have selected to apply, you can click on either **View IP NAR** or **View CLID/DNIS NAR**, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Step 4 To define and apply a NAR, for this particular user group, that permits or denies this group's access based on IP address, or IP address and port, follow these steps:

Tip You should define most NARs from within the Shared Components section so that the restrictions can be applied to more than one group or user. For more information, see the "Shared Network Access Restrictions Configuration" section on page 5-7.

a. In the Network Access Restrictions table, select the **Define IP-based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, select either **Permitted Calling/Point of Access Locations** or **Denied Calling/Point of Access Locations**.

c. Select or enter the information in the following boxes:

- **AAA Client**—Select either **All AAA Clients** or the name of the NDG or the name of the individual AAA client to which to permit or deny access.
- **Port**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports on the selected AAA client.
- **Address**—Type the IP address or addresses to filter on when performing access restrictions. You can use the wildcard asterisk (*).

d. Click **Enter**.

Result: The specified the AAA client, port, and address information appears in the NAR Access Control list.

Step 5 To permit or deny this user group's access based on calling location or values other than an established IP address, follow these steps:

a. Select the **Define CLI/DNIS-based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, select one of the following:

- **Permitted Calling/Point of Access Locations**
- **Denied Calling/Point of Access Locations**

c. From the AAA Client list, select either **All AAA Clients** or the name of the NDG or the name of the particular AAA client to which to permit or deny access.

Downloaded from www.Manualslib.com manuals search engine

d. Complete the following boxes:

Note You must make an entry in each box. You can use the wildcard asterisk (*) for all or part of a value. The format you use must match the format of the string you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

- **PORT**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports.
- **CLI**—Type the CLI number to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access based on part of the number or all numbers.

Tip This is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet client's MAC address. For more information, see the "About Network Access Restrictions" section on page 5-6.

- **DNIS**—Type the DNIS number to restrict access based on the number into which the user will be dialing. You can use the wildcard asterisk (*) to permit or deny access based on part of the number or all numbers.

Tip This is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet AP's MAC address. For more information, see the "About Network Access Restrictions" section on page 5-6.

e. Click **Enter**.

Result: The information, specifying the AAA client, Port, CLI, and DNIS appears in the list.

Downloaded from www.Manualslib.com manuals search engine

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Max Sessions for a User Group

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**. Then select the **Max Sessions** check box.

Perform this procedure to define the maximum number of sessions available to a group, or to each individual user in a group, or both. The settings are as follows:

- **Sessions available to group**—Sets the maximum number of total simultaneous connections for the entire group.
- **Sessions available to users of this group**—Sets the maximum number of total simultaneous connections for each user in this group.

Tip As an example, Sessions available to group is set to 10 and Sessions available to users of this group is set to 2. If each user is using the maximum 2 simultaneous sessions, no more than 5 users can log in.

Note A session is any type of connection supported by RADIUS or TACACS+, such as PPP, NAS prompt, Telnet, ARAP, IPX/SLIP.

Note The default setting for group Max Sessions is Unlimited for both the group and the user within the group.

Downloaded from www.Manualslib.com manuals search engine

To configure the max sessions settings for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 In the Max Sessions table, under Sessions available to group, select one of the following two options:

- **Unlimited**—Select to allow this group an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
- *n*—Type the maximum number of simultaneous sessions to allow this group.

Step 4 In the lower portion of the Max Sessions table, under Sessions available to users of this group, select one of the following two options:

- **Unlimited**—Select to allow each individual in this group an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
- *n*—Type the maximum number of simultaneous sessions to allow each individual in this group.

Note Settings made in User Setup override group settings. For more information, see the "Setting Max Sessions Options for a User" section on page 7-17.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Setting Usage Quotas for a User Group

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**. Then select the **Usage Quotas** check box.

Perform this procedure to define usage quotas for members of a group. Session quotas affect each user of a group individually, not the group collectively. You can set quotas for a given period in two ways:

- By total duration of session
- By the total number of sessions

If you make no selections in the Usage Quotas section for a group, no usage quotas are enforced on users assigned to that group, unless you configure usage quotas for the individual users.

Note The Usage Quotas section on the Group Settings page does not show usage statistics.
Usage statistics are available only on the settings page for an individual user. For more information, see the "Setting User Usage Quotas Options" section on page 7-19.

When a user exceeds his assigned quota, Cisco Secure ACS denies that user access upon attempting to start a session. If a quota is exceeded during a session, Cisco Secure ACS allows the session to continue.

You can reset the usage quota counters for all users of a group from the Group Settings page. For more information about resetting usage quota counters for a whole group, see the "Resetting Usage Quota Counters for a User Group" section on page 6-49.

Downloaded from www.Manualslib.com manuals search engine

Tip To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated when the user logs off. If the AAA client through which the user is accessing your network fails, the quota is not updated. In the case of multiple sessions, such as with ISDN, the quota is not updated until all sessions terminate, which means that a second channel will be accepted even if the first channel has exhausted the user's quota.

To set user usage quotas for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 To define usage quotas based on duration of sessions, follow these steps:

a. In the Usage Quotas table, select the **Limit User to** *x* **hours per** *time unit* check box.

b. Type the number of hours to which you want to limit group members in the **to** *x* **hours** box.
Use decimal values to indicate minutes. For example, a value of 10.5 would equal ten hours and 30 minutes.

c. Select the period for which the quota is effective from the following:

- **per Day**—From 12:01 a.m. until midnight
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month
- **Total**—An ongoing count of hours, without an end

Step 4 To define user session quotas based on number of sessions, follow these steps:

a. In the Usage Quotas table, select the **Limit each user of this group to** *x* **sessions** check box.

b. Type the number of sessions to which you want to limit users in the **to** *x* **sessions** box.

Downloaded from www.Manualslib.com manuals search engine

c. Select the period for which the session quota is effective from the following:

- **per Day**—From 12:01 a.m. until midnight
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month
- **Total**—An ongoing count of session, without an end

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuration-specific User Group Settings

This section details procedures that you perform only as applicable to your particular network security configuration. For instance, if you have no token server configured, you do not have to set token card settings for each group.

This section contains the following procedures:

- Setting Token Card Settings for a User Group, page 6-17
- Setting Enable Privilege Options for a User Group, page 6-18
- Enabling Password Aging for the CiscoSecure User Database, page 6-20
- Enabling Password Aging for Users in Windows Databases, page 6-25
- Setting IP Address Assignment Method for a User Group, page 6-26
- Assigning a Downloadable PIX ACL to a Group, page 6-27
- Configuring TACACS+ Settings for a User Group, page 6-28
- Configuring a Shell Command Authorization Set for a User Group, page 6-30
- Configuring a PIX Command Authorization Set for a User Group, page 6-32
- Configuring IETF RADIUS Settings for a User Group, page 6-34
- Configuring Cisco IOS/PIX RADIUS Settings for a User Group, page 6-36

Downloaded from www.Manualslib.com manuals search engine

- Configuring Ascend RADIUS Settings for a User Group, page 6-37
- Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group, page 6-38
- Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 6-39
- Configuring Microsoft RADIUS Settings for a User Group, page 6-41
- Configuring Nortel RADIUS Settings for a User Group, page 6-42
- Configuring Juniper RADIUS Settings for a User Group, page 6-44
- Configuring Cisco BBSM RADIUS Settings for a User Group, page 6-45

Note RADIUS (Cisco Aironet) is not an option since there are no Cisco Aironet-specific VSAs. The length of user session timeouts is controlled by IETF RADIUS attribute 27, Session-Timeout.

Note When a vendor-specific variety of RADIUS is configured for use by network devices, the RADIUS (IETF) attributes are available because they are the base set of attributes, used as the first 74 attributes for all RADIUS vendors.

The content of these subsections is dynamic and based on two factors as follows:

- For a particular protocol to be listed, a AAA client must be configured to authenticate using that protocol. For more information, see the "AAA Client Configuration" section on page 4-8.
- The specific attributes for a particular protocol must be configured for display at the group level. For more information, see the "Protocol Configuration Options for TACACS+" section on page 3-7 or the "Protocol Configuration Options for RADIUS" section on page 3-10.

Downloaded from www.Manualslib.com manuals search engine

Setting Token Card Settings for a User Group

Note If this section does not appear, configure a token server. Then click **External User Databases**, click **Database Configuration**, and then add the applicable token card server.

Perform this procedure to allow a token to be cached. This means users can use a second B channel without having to enter a second one-time password (OTP).

Caution This option is for use with token caching only for ISDN terminal adapters. You should fully understand token caching and ISDN concepts and principles before implementing this option. Token caching allows you to connect to multiple B channels without having to provide a token for each channel connection. Token card settings are applied to all users in the selected group.

Options for token caching include the following:

- **Session**—You can select Session to cache the token for the entire session. This allows the second B channel to dynamically go in and out of service.
- **Duration**—You can select Duration and specify a period of time to have the token cached (from the time of first authentication). If this time period expires, the user cannot start a second B channel.
- **Session and Duration**—You can select both Session and Duration so that, if the session runs longer than the duration value, a new token is required to open a second B channel. Type a value high enough to allow the token to be cached for the entire session. If the session runs longer than the duration value, a new token is required to open a second B channel.

To set token card settings for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **Token Cards**.

Downloaded from www.Manualslib.com manuals search engine

Step 4 In the Token Card Settings table, to cache the token for the entire session, select **Session**.

Step 5 Also in the Token Card Settings table, to cache the token for a specified time period (measured from the time of first authentication) follow these steps:

a. Select **Duration**.

b. Type the duration length in the box.

c. Select the unit of measure, either **Seconds**, **Minutes** or **Hours**.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Enable Privilege Options for a User Group

Note If this section does not appear, configure the interface to display advanced TACACS+ settings. Click **Interface Configuration**, click **TACACS+ (Cisco)**. At the bottom of the page in the Advanced Configuration Options table, select the **Advanced TACACS+ features** check box.

Perform this procedure to configure group-level TACACS+ enable parameters. The three possible TACACS+ enable options are as follows:

- **No Enable Privilege**—(default) Select this option to disallow enable privileges for this user group.
- **Max Privilege for Any AAA Client**—Select this option to select the maximum privilege level for this user group for any AAA client on which this group is authorized.
- **Define max Privilege on a per-network device group basis**—Select this option to define maximum privilege levels for a NDG. To use this option, you create a list of device groups and corresponding maximum privilege levels. See your AAA client documentation for information about privilege levels.

Downloaded from www.Manualslib.com manuals search engine

Note To define levels in this manner, you must have configured the option in Interface Configuration; if you have not done so already, click **Interface Configuration**, click **Advanced Settings**, and then select the **Network Device Groups** check box.

If you are using NDGs, this option lets you easily configure the NDG for enable-level mapping rather than having to do it for each user in the group.

To set enable privilege options for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **Enable Options**.

Step 4 Do one of the following:

a. To disallow enable privileges for this user group, select the **No Enable Privilege** option.

b. To set the maximum privilege level for this user group, for any ACS on which this group is authorized, select the **Max Privilege for Any Access Server** option. Then select the maximum privilege level from the list.

c. To define this user group's maximum privilege level for a NDG, select the **Define max Privilege on a per-network device group basis** option. Then, from the lists, select the NDG and a corresponding privilege level. Finally, click **Add Association**.

Result: The association of NDG and maximum privilege level appears in the table.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Enabling Password Aging for the CiscoSecure User Database

The password aging feature of Cisco Secure ACS enables you to force users to change their passwords under one or more of the following conditions:

- After a specified number of days (age-by-date rules)
- After a specified number of logins (age-by-uses rules)
- The first time a new user logs in (password change rule)

Varieties of Password Aging Supported by Cisco Secure ACS

Cisco Secure ACS supports three distinct password aging mechanisms, as follows:

- **Windows NT/2000 Password Aging**—Users must be in the Windows NT/2000 database and be using the Windows Dial-up Networking (DUN) client. For information on the requirements and configuration of this password aging mechanism, see the "Enabling Password Aging for Users in Windows Databases" section on page 6-25.
- **Password Aging for Device-hosted Sessions**—Users must be in the CiscoSecure user database, the AAA client must be running TACACS+, and the connection must use Telnet.
- **Password Aging for Transit Sessions**—Users must be in the CiscoSecure user database. Users must be using the Windows 95/98/ME, Windows NT 3.51, Windows NT 4.0, Windows 2000 DUN client, or another PPP dialup client. Further, the end-user client must have CiscoSecure Authentication Agent (CAA) installed in Windows 95/98/ME or Windows NT/2000.

Tip The CAA software is available at http://www.cisco.com.

Also, to run password aging for transit sessions, the AAA client can be running either RADIUS or TACACS+; and the AAA client must be using Cisco IOS Release 11.2.7 or later and be configured to send a "watchdog" accounting packet (aaa accounting new-info update) with the IP address of the calling station. (Watchdog packets are interim packets sent periodically during a session. They enable an approximation of session length in the event that the AAA client fails and, thereby, no stop packet is received to mark the end of the session.)

Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS supports password aging using the RADIUS protocol under MS CHAP versions 1 and 2. Cisco Secure ACS does not support password aging over Telnet connections using the RADIUS protocol.

Caution If a user employing a RADIUS connection tries to make a Telnet connection to the AAA client during or after the password aging warning or grace period, the change password option does not appear, and the user's account is expired.

Password Aging Feature Settings

This section details only the Password Aging for Device-hosted Sessions and Password Aging for Transit Sessions mechanisms. For information on the Windows NT/2000 Password Aging mechanism and the Windows 2000 DUN client, see the "Enabling Password Aging for Users in Windows Databases" section on page 6-25.

The password aging feature in Cisco Secure ACS has the following major and minor options:

- **Apply age-by-date rules**—Selecting this check box configures Cisco Secure ACS to determine password aging by date. The age-by-date rules contain the following settings:
  - **Active period**—The number of days users will be allowed to log in before being prompted to change their passwords. For example, if you enter 20, users can use their passwords for 20 days without being prompted to change them. The default Active period is 20 days.
  - **Warning period**—The number of days users will be notified to change their passwords. The user's existing password can be used, but the Cisco Secure ACS presents a warning indicating that the password must be changed and displays the number of days left before the password expires. For example, if you enter 5 in this box and 20 in the Active period box, users will be notified to change their passwords on the 21st through 25th days.
  - **Grace period**—The number of days to provide as the users' grace period. The grace period allows a user to log in once to change the password. The existing password can be used one last time after the number of days specified in the active and warning period fields has been exceeded. Then, a dialog box warns the user that the account will be

Downloaded from www.Manualslib.com manuals search engine

disabled if the password is not changed, and enables the user to change it. Continuing with the examples above, if you allow a 5-day grace period, a user who did not log in during the active and warning periods would be permitted to change passwords up to and including the 30th day. However, even though the grace period is set for 5 days, a user is allowed only one attempt to change the password when the password is in the grace period. Cisco Secure ACS displays the "last chance" warning only once. If the user does not change the password, this login is still permitted, but the password expires, and the next authentication is denied. An entry is logged in the Failed-Attempts log, and the user must contact an administrator to have the account reinstated.

Note All passwords expire at midnight, not the time at which they were set.

- **Apply age-by-uses rules**—Selecting this check box configures Cisco Secure ACS to determine password aging by the number of logins. The age-by-uses rules contain the following settings:
  - **Issue warning after** *x* **logins**—The number of the login upon which Cisco Secure ACS begins prompting users to change their passwords. For example, if you enter 10, users are allowed to log in 10 times without a change-password prompt. On the 11th login, they are prompted to change their passwords.

Tip To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

  - **Require change after** *x* **logins**—The number of the login upon which to notify users that they must to change their passwords. Continuing with the previous example, if this number is 12, users receive prompts requesting them to change their passwords on their 11th and 12th logins. On the 13th login, they receive a prompt telling them that they must change their passwords. If users do not change their passwords now, their accounts expire and they cannot log in. This number must be greater than the Issue warning after *x* login number.

Downloaded from www.Manualslib.com manuals search engine

Tip To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

- **Apply password change rule**—Selecting this check box forces new users to change their password the first time they log in.
- **Generate greetings for successful logins—**Selecting this check box enables a "Greetings" message to display whenever users log in successfully via the CAA client. The message contains up-to-date password information specific to this user's account.

The password aging rules are not mutually exclusive; a rule is applied for each check box that is selected. For example, users can be forced to change their passwords every 20 days, and every 10 logins, and to receive warnings and grace periods accordingly.

If no options are checked, passwords never expire.

Unlike most other parameters, which have corresponding settings at the user level, password aging parameters are configured only on a group basis.

Users who fail authentication because they have not changed their passwords and have exceeded their grace periods are logged in the Failed Attempts log. The accounts are expired and appear in the Accounts Disabled list.

Before You Begin

- Verify that your AAA client is running the TACACS+ or RADIUS protocol. (TACACS+ only supports password aging for device-hosted sessions.)
- Set up your AAA client to perform authentication *and* accounting using the same protocol, either TACACS+ RADIUS.
- Set up your AAA client to use Cisco IOS Release 11.2.7 or later and to send a watchdog accounting packet (aaa accounting new-info update) with the IP address of the calling station.

To set password aging rules for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Downloaded from www.Manualslib.com manuals search engine

Step 3 From the Jump To list at the top of the page, choose **Password Aging**.

Result: The Password Aging Rules table appears.

Step 4 To set password aging by date, select the **Apply age-by-date rules** check box and type the number of days for the following options, as applicable:

- Active period
- Warning period
- Grace period

Step 5 To set password aging by use, select the **Apply age-by-uses rules** check box and type the number of logins for each of the following options, as applicable:

- Issue warning after *x* logins
- Require change after *x* logins

Step 6 To force the user to change the password on the first login after an administrator has changed it, select the **Apply password change rule** check box.

Step 7 To enable a "Greetings" message display, select the **Generate greetings for successful logins** check box.

Step 8 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 9 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Enabling Password Aging for Users in Windows Databases

The Windows NT/2000 Password Aging mechanism is separate and distinct from the other Cisco Secure ACS password aging mechanisms. For information on the requirements and settings for the password aging mechanisms that control users in the CiscoSecure user database, see the "Enabling Password Aging for the CiscoSecure User Database" section on page 6-20. Requirements for implementing the Windows NT/2000 Password Aging mechanism include the following:

- Communication between Cisco Secure ACS and the AAA client must use RADIUS.
- The AAA client must support MS CHAP password aging in addition to MS CHAP authentication.
- Users must be in a Windows NT/2000 database.
- Users must use the Windows DUN client.
- You must enable MS CHAP version 1 or MS CHAP version 2, or both, in the Windows NT/2000 configuration within the External User Databases section. (Cisco IOS devices support password aging only in MS CHAP version 2.)

Tip For information on enabling MS CHAP for password changes, see the "Configuring a Windows NT/2000 External User Database" section on page 11-13. For information on enabling MS CHAP in System Configuration, see the "Global Authentication Setup" section on page 8-73.

Note You can run both the Windows NT/2000 Password Aging and the Cisco Secure ACS Password Aging for Transit Sessions mechanisms, concurrently, provided that the users authenticate from the two different databases.

Users whose Windows accounts reside in "remote" domains (that is, not the domain within which Cisco Secure ACS is running) can only use the Windows-based password aging if they supply their domain name.

Downloaded from www.Manualslib.com manuals search engine

The methods and functionality of Windows password aging differ according to whether you are using Windows NT or Windows 2000, and whether you employ Active Directory (AD) or Security Accounts Manager (SAM). Setting password aging for users in the Windows NT/2000 database is only one part of the larger task of setting security policies in Windows. For comprehensive information on Windows procedures, refer to your Windows NT/2000 system documentation.

Setting IP Address Assignment Method for a User Group

Perform this procedure to configure the way Cisco Secure ACS assigns IP addresses to the users in the group. The four possible methods are as follows:

- **No IP address assignment**—No IP address is assigned to this group.
- **Assigned by dialup client**—Use the IP address that is configured on the dialup client's network settings for TCP/IP.
- **Assigned from AAA Client pool**—The IP address is assigned by an IP address pool assigned on the AAA client.
- **Assigned from AAA server pool**—The IP address is assigned by an IP address pool assigned on the AAA server.

To set an IP address assignment method for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **IP Address Assignment**.

Step 4 In the IP Assignment table, do one of the following:

a. Select **No IP address assignment**.

b. Select **Assigned by dialup client**.

c. Select **Assigned from AAA Client pool**. Then, type the AAA client IP pool name.

d. Select **Assigned from AAA pool**. Then, select the AAA server IP pool name in the Available Pools list and click —> (right arrow button) to move the name into the Selected Pools list.

Downloaded from www.Manualslib.com manuals search engine

Note If there is more than one pool in the Selected Pools list, the users in this group are assigned to the first available pool in the order listed.

Tip To change the position of a pool in the list, select the pool name and click **Up** or **Down** until the pool is in the position you want.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Assigning a Downloadable PIX ACL to a Group

The Downloadable ACLs feature enables you to assign a PIX Access Control List (ACL) at the group level.

Note You must have established one or more PIX ACLs before attempting to assign one. For instructions on how to add a downloadable PIX ACL using the Shared Profile Components section of the Cisco Secure ACS HTML interface, see the "Adding a Downloadable PIX ACL" section on page 5-3.

Tip The Downloadable ACLs table does not appear if it has not been enabled. To enable the Downloadable ACLs table, click **Interface Configuration**, click **Advanced Options**, and then select the **Group-Level Downloadable ACLs** check box.

Downloaded from www.Manualslib.com manuals search engine

To assign a downloadable PIX ACL to a group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **Downloadable ACLs**.

Step 4 Under the Downloadable ACLs section, click the **Assign PIX ACL** check box.

Step 5 Select a PIX ACL from the list.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring TACACS+ Settings for a User Group

Perform this procedure to configure and enable the service/protocol parameters to be applied for the authorization of each user who belongs to the group. For information on how to configure settings for the Shell Command Authorization Set, see the "Configuring a Shell Command Authorization Set for a User Group" section on page 6-30.

Note To display or hide additional services or protocols, click **Interface Configuration**, click **TACACS+ (Cisco IOS)**, and then select or clear items in the group column, as applicable.

Downloaded from www.Manualslib.com manuals search engine

To configure TACACS+ settings for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

Result: The system displays the TACACS+ Settings table section.

Step 4 To configure services and protocols in the TACACS+ Settings table to be authorized for the group, follow these steps:

a. Select the check box next to the service/protocol (for example, PPP IP).

b. Under each service/protocol that you selected in the previous step, select attributes and then type in the corresponding values, as applicable, to further define authorization for that service/protocol.

For more information about attributes, see Appendix C, "TACACS+ Attribute-Value Pairs," or your AAA client documentation.

Tip For access control lists (ACLs) and IP address pools, the name of the ACL or pool as defined on the AAA client should be entered. (An ACL is a list of Cisco IOS commands used to restrict access to or from other devices and users on the network.)

Note Leave the box blank if the default (as defined on the AAA client) should be used.

Note You can define and download an ACL. Click **Interface Configuration**, click **TACACS+ (Cisco IOS)**, and then select **Display a window for each service selected in which you can enter customized TACACS+ attributes**. A box opens under each service/protocol in which you can define an ACL.

Downloaded from www.Manualslib.com manuals search engine

Step 5 To allow all services to be permitted unless specifically listed and disabled, you can select the **Default (Undefined) Services** check box under the Checking this option will PERMIT all UNKNOWN Services table.

Warning **This is an advanced feature and should only be used by administrators who understand the security implications.**

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring a Shell Command Authorization Set for a User Group

Use this procedure to specify the shell command authorization set parameters for a group. There are four basic options:

- **None**—No authorization for shell commands
- **Assign a Shell Command Authorization Set for any network device**—One shell command authorization set is assigned, and it applies to all network devices
- **Assign a Shell Command Authorization Set on a per Network Device Group Basis**—Enables you to associate particular shell command authorization sets to be effective on particular NDGs
- **Per Group Command Authorization**—Enables you to permit or deny specific Cisco IOS commands and arguments at the group level

Note This feature requires that you have previously configured a shell command authorization set. For detailed steps, see the "Command Authorization Sets Configuration" section on page 5-14.

Downloaded from www.Manualslib.com manuals search engine

To specify shell command authorization set parameters for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

Result: The system displays the TACACS+ Settings table section.

Step 4 Use the vertical scroll bar to scroll to the Shell Command Authorization Set feature area.

Step 5 To prevent the application of any shell command authorization set, select (or accept the default of) the **None** option.

Step 6 To assign a particular shell command authorization set to be effective on any configured network device, follow these steps:

a. Select the **Assign a Shell Command Authorization Set for any network device** option.

b. Then, from the list directly below that option, select the shell command authorization set you want applied to this group.

Step 7 To create associations that assign a particular shell command authorization set to be effective on a particular NDG, for each association, follow these steps:

a. Select the **Assign a Shell Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and a corresponding **Command Set**.

c. Click **Add Association**.

Result: The associated NDG and shell command authorization set appear in the table.

Step 8 To define the specific Cisco IOS commands and arguments to be permitted or denied at the group level, follow these steps:

a. Select the **Per Group Command Authorization** option.

b. Under Unmatched Cisco IOS commands, select either **Permit** or **Deny**.

Downloaded from www.Manualslib.com manuals search engine

If you select Permit, users can issue all commands not specifically listed. If you select Deny, users can issue only those commands listed.

c. To list particular commands to be permitted or denied, select the **Command** check box and then type the name of the command, define its arguments using standard permit or deny syntax, and select whether unlisted arguments should be permitted or denied.

Warning **This is a powerful, advanced feature and should be completed by an administrator skilled with Cisco IOS commands. Correct syntax is the administrator's responsibility. For information on how Cisco Secure ACS employs pattern matching in command arguments, see the "About Pattern Matching" section on page 5-14.**

Tip To enter several commands, you must click **Submit** after specifying a command. A new command entry box appears below the box you just completed.

Configuring a PIX Command Authorization Set for a User Group

Use this procedure to specify the PIX command authorization set parameters for a user group. There are three basic options:

- **None**—No authorization for PIX commands
- **Assign a PIX Command Authorization Set for any network device**—One PIX command authorization set is assigned, and it applies all network devices
- **Assign a PIX Command Authorization Set on a per Network Device Group Basis**—Particular PIX command authorization sets are to be effective on particular NDGs

Downloaded from www.Manualslib.com manuals search engine

Before You Begin

- Ensure that a AAA client has been configured to use TACACS+ as the security control protocol.
- In the TACACS+ (Cisco) section of Interface Configuration, ensure that the PIX Shell (pixShell) option is selected in the Group column.
- Ensure that you have previously configured one or more PIX command authorization sets. For detailed steps, see the "Command Authorization Sets Configuration" section on page 5-14.

To specify PIX command authorization set parameters for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

Result: The system displays the TACACS+ Settings table section.

Step 4 Scroll down to the PIX Command Authorization Set feature area within the TACACS+ Settings table.

Step 5 To prevent the application of any PIX command authorization set, select (or accept the default of) the **None** option.

Step 6 To assign a particular PIX command authorization set to be effective on any configured network device, follow these steps:

a. Select the **Assign a PIX Command Authorization Set for any network device** option.

b. From the list directly below that option, select the PIX command authorization set you want applied to this user group.

Downloaded from www.Manualslib.com manuals search engine

Step 7 To create associations that assign a particular PIX command authorization set to be effective on a particular NDG, for each association, follow these steps:

a. Select the **Assign a PIX Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and an associated **Command Set**.

c. Click **Add Association**.

Result: The associated NDG and PIX command authorization set appear in the table.

Note To remove or edit an existing PIX command authorization set association, you can select the association from the list and then click **Remove Association**.

Configuring IETF RADIUS Settings for a User Group

These parameters appear only when both the following are true:

- A AAA client has been configured to use one of the RADIUS protocols in Network Configuration.
- Group-level RADIUS attributes have been enabled in Interface Configuration: RADIUS (IETF).

RADIUS attributes are sent as a profile for each user from Cisco Secure ACS to the requesting AAA client. To display or hide any of these attributes, see the "Protocol Configuration Options for RADIUS" section on page 3-10. For a list and explanation of RADIUS attributes, see Appendix D, "RADIUS Attributes." For more information about how your AAA client uses RADIUS, refer to your AAA client vendor documentation.

Downloaded from www.Manualslib.com manuals search engine

To configure IETF RADIUS attribute settings to be applied as an authorization for each user in the current group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **RADIUS (IETF)**.

Step 4 For each IETF RADIUS attribute you need to authorize for the current group, select the check box next to the attribute and then further define the authorization for the attribute in the field or fields next to it.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 6 To configure the vendor-specific attributes (VSAs) for any RADIUS network device vendor supported by Cisco Secure ACS, see the appropriate section:

- Configuring Cisco IOS/PIX RADIUS Settings for a User Group, page 6-36
- Configuring Ascend RADIUS Settings for a User Group, page 6-37
- Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group, page 6-38
- Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 6-39
- Configuring Microsoft RADIUS Settings for a User Group, page 6-41
- Configuring Nortel RADIUS Settings for a User Group, page 6-42
- Configuring Juniper RADIUS Settings for a User Group, page 6-44
- Configuring Cisco BBSM RADIUS Settings for a User Group, page 6-45

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Configuring Cisco IOS/PIX RADIUS Settings for a User Group

The Cisco IOS/PIX RADIUS parameters appear only when both the following are true:

- A AAA client has been configured to use RADIUS (Cisco IOS/PIX) in Network Configuration.
- Group-level RADIUS (Cisco IOS/PIX) attributes have been enabled in Interface Configuration: RADIUS (Cisco IOS/PIX).

Cisco IOS/PIX RADIUS represents only the Cisco VSAs. You must configure both the IETF RADIUS and Cisco IOS/PIX RADIUS attributes.

Note To hide or display Cisco IOS/PIX RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Cisco IOS/PIX)" section on page 3-14.

To configure and enable Cisco IOS/PIX RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Before you configure Cisco IOS/PIX RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see the "Configuring IETF RADIUS Settings for a User Group" section on page 6-34.

Step 2 For the Cisco attributes, determine the attributes to be authorized for the group by selecting the check box next to the attribute, and then type the commands (such as TACACS+ commands) to be packed as a RADIUS VSA.

Step 3 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 4 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Configuring Ascend RADIUS Settings for a User Group

The Ascend RADIUS parameters appear only when both the following are true:

- A AAA client has been configured to use RADIUS (Ascend) or RADIUS (Cisco IOS/PIX) in Network Configuration.
- Group-level RADIUS (Ascend) attributes have been enabled in Interface Configuration: RADIUS (Ascend).

Ascend RADIUS represents only the Ascend proprietary attributes. You must configure both the IETF RADIUS and Ascend RADIUS attributes. Proprietary attributes override IETF attributes.

The default attribute setting displayed for RADIUS is `Ascend-Remote-Addr`.

Note To hide or display Ascend RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Ascend)" section on page 3-14.

To configure and enable Ascend RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see the "Configuring IETF RADIUS Settings for a User Group" section on page 6-34.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Ascend)**.

Step 5 In the Ascend RADIUS Attributes table, determine the attributes to be authorized for the group by selecting the check box next to the attribute. Be sure to further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix D, "RADIUS Attributes," or your AAA client documentation.

Downloaded from www.Manualslib.com manuals search engine

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group

The Cisco VPN 3000 Concentrator RADIUS attribute configurations appear only if both the following are true:

- A AAA client has been configured to use RADIUS (Cisco VPN 3000) in Network Configuration.
- Group-level RADIUS (Cisco VPN 3000) attributes have been enabled on the RADIUS (Cisco VPN 3000) page of the Interface Configuration section.

Cisco VPN 3000 Concentrator RADIUS represents only the Cisco VPN 3000 Concentrator VSAs. You must configure both the IETF RADIUS and Cisco VPN 3000 Concentrator RADIUS attributes.

Note To hide or display Cisco VPN 3000 Concentrator RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Cisco VPN 3000)" section on page 3-15.

To configure and enable Cisco VPN 3000 Concentrator RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see the "Configuring IETF RADIUS Settings for a User Group" section on page 6-34.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Downloaded from www.Manualslib.com manuals search engine

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 3000)**.

Step 5 In the Cisco VPN 3000 Concentrator RADIUS Attributes table, determine the attributes to be authorized for the group by selecting the check box next to the attribute. Further define the authorization for that attribute in the field next to it.

For more information about attributes, see Appendix D, "RADIUS Attributes," or the documentation for network devices using RADIUS.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group

The Cisco VPN 5000 Concentrator RADIUS attribute configurations display only when both the following are true:

- A network device has been configured to use RADIUS (Cisco VPN 5000) in Network Configuration.
- Group-level RADIUS (Cisco VPN 5000) attributes have been enabled on the RADIUS (Cisco VPN 5000) page of the Interface Configuration section.

Cisco VPN 5000 Concentrator RADIUS represents only the Cisco VPN 5000 Concentrator VSAs. You must configure both the IETF RADIUS and Cisco VPN 5000 Concentrator RADIUS attributes.

Note To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Cisco VPN 5000)" section on page 3-16.

Downloaded from www.Manualslib.com manuals search engine

To configure and enable Cisco VPN 5000 Concentrator RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see the "Configuring IETF RADIUS Settings for a User Group" section on page 6-34.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 5000)**.

Step 5 In the Cisco VPN 5000 Concentrator RADIUS Attributes table, select the attributes that should be authorized for the group by selecting the check box next to the attribute. Further define the authorization for each attribute in the field next to it.

For more information about attributes, see Appendix D, "RADIUS Attributes," or the documentation for network devices using RADIUS.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Configuring Microsoft RADIUS Settings for a User Group

Microsoft RADIUS provides VSAs supporting MPPE, which is an encryption technology developed by Microsoft to encrypt PPP links. These PPP connections can be via a dial-in line, or over a VPN tunnel. The Microsoft RADIUS attribute configurations appear only when both the following are true:

- A network device has been configured in Network Configuration that uses a RADIUS protocol that supports the Microsoft RADIUS VSA.
- Group-level Microsoft RADIUS attributes have been enabled on the RADIUS (Microsoft) page of the Interface Configuration section.

The following Cisco Secure ACS RADIUS protocols support the Microsoft RADIUS VSA:

- Cisco IOS/PIX
- Cisco VPN 3000
- Ascend

Microsoft RADIUS represents only the Microsoft VSA. You must configure both the IETF RADIUS and Microsoft RADIUS attributes.

Note To hide or display Microsoft RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Microsoft)" section on page 3-17.

To configure and enable Microsoft RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see the "Configuring IETF RADIUS Settings for a User Group" section on page 6-34.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Microsoft)**.

Downloaded from www.Manualslib.com manuals search engine

Step 5 In the Microsoft RADIUS Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix D, "RADIUS Attributes," or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is generated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Nortel RADIUS Settings for a User Group

The Nortel RADIUS attribute configurations appear only when both the following are true:

- A network device has been configured in Network Configuration that uses a RADIUS protocol that supports the Nortel RADIUS VSA.
- Group-level Nortel RADIUS attributes have been enabled on the RADIUS (Nortel) page of the Interface Configuration section.

Nortel RADIUS represents only the Nortel VSA. You must configure both the IETF RADIUS and Nortel RADIUS attributes.

Note To hide or display Nortel RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Nortel)" section on page 3-18.

Downloaded from www.Manualslib.com manuals search engine

To configure and enable Nortel RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see the Configuring IETF RADIUS Settings for a User Group, page 6-34.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Nortel)**.

Step 5 In the Nortel RADIUS Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix D, "RADIUS Attributes," or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is generated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Configuring Juniper RADIUS Settings for a User Group

Juniper RADIUS represents only the Juniper VSAs. You must configure both the IETF RADIUS and Juniper RADIUS attributes.

Note To hide or display Juniper RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Juniper)" section on page 3-19.

To configure and enable Juniper RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see the "Configuring IETF RADIUS Settings for a User Group" section on page 6-34.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Juniper)**.

Step 5 In the Juniper RADIUS Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix D, "RADIUS Attributes," or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is generated by Cisco Secure ACS; there is no value to set in the HTML interface.

Downloaded from www.Manualslib.com manuals search engine

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco BBSM RADIUS Settings for a User Group

Cisco BBSM RADIUS represents only the Cisco BBSM RADIUS VSAs. You must configure both the IETF RADIUS and Cisco BBSM RADIUS attributes.

Note To hide or display Cisco BBSM RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Cisco BBSM)" section on page 3-20.

To configure and enable Cisco BBSM RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see the "Configuring IETF RADIUS Settings for a User Group" section on page 6-34.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco BBSM)**.

Downloaded from www.Manualslib.com manuals search engine

Step 5 In the Cisco BBSM RADIUS Attributes table, specify the attribute to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix D, "RADIUS Attributes," or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is generated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Custom RADIUS VSA Settings for a User Group

User-defined, custom Radius VSA configurations appear only when all the following are true:

- You have defined and configured the custom RADIUS VSAs. (For information about creating user-defined RADIUS VSAs, see the "User-Defined RADIUS Vendors and VSA Sets" section on page E-27.)
- A network device has been configured in Network Configuration that uses a RADIUS protocol that supports the custom VSA.
- Group-level custom RADIUS attributes have been enabled on the RADIUS (*Name*) page of the Interface Configuration section.

You must configure both the IETF RADIUS and the custom RADIUS attributes.

Downloaded from www.Manualslib.com manuals search engine

To configure and enable custom RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see the "Configuring IETF RADIUS Settings for a User Group" section on page 6-34.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (***custom name***)**.

Step 5 In the RADIUS (*custom name*) Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix D, "RADIUS Attributes," or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is generated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see the "Saving Changes to User Group Settings" section on page 6-50.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Group Setting Management

This section describes how to use the Cisco Secure ACS Group Setup section to perform a variety of managerial tasks.

This section contains the following procedures:

- Listing Users in a User Group, page 6-48
- Resetting Usage Quota Counters for a User Group, page 6-49
- Renaming a User Group, page 6-49
- Saving Changes to User Group Settings, page 6-50

Listing Users in a User Group

To list all users in a specified group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select the group.

Step 3 Click **Users in Group**.

Result: The User List page opens in the display area.

Step 4 To open a user account (to view, modify, or delete a user), click the name of the user in the User List.

Downloaded from www.Manualslib.com manuals search engine

Resetting Usage Quota Counters for a User Group

You can reset the usage quota counters for all members of a group, either before or after a quota has been exceeded.

To reset usage quota counters for all members of a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select the group.

Step 3 In the Usage Quotas section, select the **On submit reset all usage counters for all users of this group** check box.

Step 4 Click **Submit** at the bottom of the browser page.

Result: The usage quota counters for all users in the group are reset. The Group Setup Select page appears.

Renaming a User Group

To rename a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select the group.

Step 3 Click **Rename Group**.

Result: The Renaming Group: *Group Name* page appears.

Step 4 Type the new name in the **Group** field. Group names cannot contain angle brackets (< or >).

Downloaded from www.Manualslib.com manuals search engine

Step 5 Click **Submit**.

Note The group remains in the same position in the list. The number value of the group is still associated with this group name. Some utilities, such as the database import utility, use the numeric value associated with the group.

Result: The Select page opens with the new group name selected.

Saving Changes to User Group Settings

After you have completed configuration for a group, be sure to save your work.

To save the configuration for the current group, follow these steps:

Step 1 To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, and then click **Service Control**, and click **Restart**.

Tip To save your changes and apply them immediately, click **Submit + Restart**.

Result: The group attributes are applied and services are restarted. The Edit page opens.

Note Restarting the service clears the Logged-in User Report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter.

Step 2 To verify that your changes were applied, select the group and click **Edit Settings**. View the settings.

Downloaded from www.Manualslib.com manuals search engine

Setting Up and Managing User Accounts

This chapter provides information about setting up and managing user accounts in Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS).

Note Settings at the user level override settings configured at the group level.

Before you configure User Setup, it is important to understand how this section functions. Cisco Secure ACS dynamically builds the User Setup section interface depending on the configuration of your AAA client and the security protocols being used. That is, what you see under User Setup is affected by two factors:

- Your system configuration
- Your settings in the Interface Configuration section

This chapter contains the following sections:

- **User Setup Features and Functions, page 7-2**—An overview of the User Setup section functionality.
- **About User Databases, page 7-3**—Information regarding user databases.
- **Basic User Setup Options, page 7-4**—Information and step-by-step procedures regarding the many basic settings and options that are available when configuring a user account in the Cisco Secure ACS.

Downloaded from www.Manualslib.com manuals search engine

- **Advanced User Authentication Settings, page 7-23**—Details on the steps necessary to configure a user account for authentication outside the system using the TACACS+ or RADIUS protocol options.
- **User Management, page 7-51**—Information about viewing, disabling, and resetting user accounts.

User Setup Features and Functions

The User Setup section of the Cisco Secure ACS HTML interface is the centralized location for all operations regarding user account configuration and administration.

From within the User Setup section, you can perform the following tasks:

- View a list of all users in the CiscoSecure user database
- Find a user
- Add a user
- Assign the user to a group, including Voice over IP (VoIP) Groups
- Edit user account information
- Establish or change user authentication type
- Configure callback information for the user
- Set network access restrictions (NARs) for the user
- Configure Advanced Settings
- Set the maximum number of concurrent sessions (Max Sessions) for the user
- Disable or re-enable the user account
- Delete the user

Downloaded from www.Manualslib.com manuals search engine

About User Databases

Cisco Secure ACS authenticates users against one of several possible databases, including its CiscoSecure user database. Regardless of which database you configure Cisco Secure ACS to use when authenticating a user, all users have accounts within the CiscoSecure user database, and authorization of users is always performed against the user records in the CiscoSecure user database.

- **CiscoSecure user database**—Authenticates a user from the local CiscoSecure user database. For more information, see the "CiscoSecure User Database" section on page 11-2.

Tip The following authentication types appear in the HTML interface only when the corresponding external user database has been configured in the Database Configuration area of the External User Databases section.

- **Windows NT/2000**—Authenticates a user with an existing account in the Windows NT/2000 user database located in the local domain or in domains configured in the Windows NT/2000 user database. For more information, see the "Windows NT/2000 User Database" section on page 11-6.
- **Generic LDAP**—Authenticates a user from a Generic LDAP external user database. For more information, see the "Generic LDAP" section on page 11-14.
- **Novell NDS**—Authenticates a user using Novell NetWare Directory Services (NDS). For more information, see the "Novell NDS Database" section on page 11-24.
- **ODBC Database**—Authenticates a user from an Open Database Connectivity-compliant database server. For more information, see the "ODBC Database" section on page 11-30.
- **LEAP Proxy RADIUS Server Database**—Authenticates a user from an LEAP Proxy RADIUS server. For more information, see the "LEAP Proxy RADIUS Server Database" section on page 11-44.
- **Token Server**—Authenticates a user from a token server database. Cisco Secure ACS supports the use of a variety of token servers for the increased security provided by one-time passwords. For more information, see the "Token Server User Databases" section on page 11-47

Downloaded from www.Manualslib.com manuals search engine

Basic User Setup Options

This section presents the basic activities you perform when configuring a new user. At its most basic level, configuring a new user requires only three steps, as follows:

- Specify a name
- Specify either a method for remote password authentication or, for authentication via the CiscoSecure user database, a password
- Submit the information

For detailed procedural information, see the "Adding a Basic User Account" section on page 7-5.

What other procedures you perform when setting up new user accounts is a function both of the complexity of your network and of the granularity of control you desire. The other basic procedures detailed in this section include the following:

- Setting Supplementary User Information, page 7-7
- Setting a Separate CHAP/MS-CHAP/ARAP Password, page 7-8
- Assigning a User to a Group, page 7-9
- Setting User Callback Option, page 7-10
- Assigning a User to a Client IP Address, page 7-11
- Setting Network Access Restrictions for a User, page 7-12
- Setting Max Sessions Options for a User, page 7-17
- Setting User Usage Quotas Options, page 7-19
- Setting Options for User Account Disablement, page 7-21
- Assigning a PIX ACL to a User, page 7-22

Beyond these basic user setup options, there are also procedures for configuring a user account for authentication via TACACS+ and RADIUS; these procedures are located under the "Advanced User Authentication Settings" section on page 7-23.

Downloaded from www.Manualslib.com manuals search engine

Note The steps for editing user account settings are essentially identical to those used when adding a user account but, to edit, you navigate directly to the field or fields to be changed. You can not edit the name associated with a user account; to change a user name you must delete the user account and establish another.

Bear in mind two things when setting up new user accounts:

- You must have configured a AAA client or external database to assign a user to it
- You must enable most options from within the Interface Configuration section for them to appear in User Setup.

Adding a Basic User Account

This procedure details the minimum steps necessary to add a new user account to the CiscoSecure user database.

To add a user account, follow these steps:

Step 1 In the navigation bar, click **User Setup**.

Result: The User Setup Select page opens.

Step 2 Type a name in the User box.

Note The username can contain up to 32 characters. Names cannot contain the following special characters:
? " * > <
Leading and trailing spaces are not allowed.

Step 3 Click **Add/Edit**.

Result: The User Setup Edit page opens. The username being added appears at the top of the page.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Ensure that the Account Disabled check box is *not* selected.

Note Alternatively, you can select the **Account Disabled** check box to create a user account that is disabled, and enable the account at another time.

Step 5 Under Password Authentication in the User Setup table, select the applicable authentication type from the list.

Tip The authentication types that appear reflect the databases that you have configured in the Database Configuration area of the External User Databases section.

Step 6 Specify a single CiscoSecure PAP password by typing it in the first set of **Password** and **Confirm Password** boxes.

Tip The CiscoSecure PAP password is also used for CHAP/MS-CHAP/ARAP if the Separate CHAP/MS-CHAP/ARAP check box is not selected.

Tip You can configure the AAA client to ask for a PAP password first and then a CHAP or MS-CHAP password so that when users dial in using a PAP password, they will authenticate. For example, the following line in the AAA client configuration file causes the AAA client to enable CHAP after PAP:
ppp authentication pap chap

Downloaded from www.Manualslib.com manuals search engine

Step 7 Do one of the following:

a. To finish configuring the user account options and establish the user account, click **Submit**.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Tip For lengthy account configurations, you can click **Submit** before continuing. This will prevent loss of information you have already entered if an unforeseen problem occurs.

Setting Supplementary User Information

Supplementary User Information can contain up to five fields that you configure. The default configuration comprises two fields: Real Name and Description.

For information about how to display and configure these optional fields, see the "User Data Configuration Options" section on page 3-3.

To enter optional information into the Supplementary User Information table, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Complete each box that appears in the Supplementary User Info table.

Step 3 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Setting a Separate CHAP/MS-CHAP/ARAP Password

Setting a separate CHAP/MS-CHAP/ARAP password adds more security to Cisco Secure ACS authentication. However, you must have a AAA client configured to support the separate password.

To allow the user to authenticate using a CHAP, MS-CHAP, or ARAP password, instead of the PAP password in the CiscoSecure user database, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Select the **Separate CHAP/MS-CHAP/ARAP** check box in the User Setup table.

Step 3 Specify the CHAP/MS-CHAP/ARAP password to be used by typing it in each of the second set of Password/Confirm boxes under the Separate (CHAP/MS-CHAP/ARAP) check box.

Note These Password and Confirm Password boxes are only required for authentication by the Cisco Secure ACS database. Additionally, if a user is assigned to a VoIP (null password) group, and the optional password is also included in the user profile, the password is not used until the user is re-mapped to a non-VoIP group.

Step 4 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Assigning a User to a Group

A user can only belong to one group in Cisco Secure ACS. The user inherits the attributes and operations assigned to his or her group. However, in the case of conflicting settings, the settings at the user level override the settings configured at the group level.

By default, users are assigned to the Default Group. Users who authenticate via the Unknown User method and who are not mapped to an existing Cisco Secure ACS group are also assigned to the Default Group.

To assign a user to a group, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 From the Group to which user is assigned list in the User Setup table, select the group to which you want to assign the user.

Step 3 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Setting User Callback Option

Callback is a command string that is passed to the access server. You can use a callback string to initiate a modem to call the user back on a specific number for added security or reversal of line charges.

To set the user callback option, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Under Callback in the User Setup table, select the applicable option. Choices include the following:

- **Use group setting**—Select if you want this user to use the setting for the group.
- **No callback allowed**—Select to disable callback for this user.
- **Callback using this number**—Select and type the complete number, including area code if necessary, on which to always call back this user.
- **Dialup client specifies callback number**—Select to enable the Windows 95/98/ME or Windows NT/2000 dialup client to specify the callback number.
- **Use Microsoft NT/2000 callback settings**—Select to use the settings specified for Windows NT/2000 callback. Note that, if a Windows account for a user resides in a remote domain, the domain in which Cisco Secure ACS resides must have a two-way trust with that domain for the Microsoft NT/2000 callback settings to operate for that user.

Note The dial-in user must have configured software that supports callback.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Assigning a User to a Client IP Address

To assign a user to a client IP address, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Under Client IP Address Assignment in the User Setup table, select the applicable option. Choices include the following:

Note The IP address assignment in User Setup overrides the IP address assignment in Group Setup.

- **Use group settings**—Select this option to use the IP address group assignment.
- **No IP address assignment**—Select this option to override the group setting if you do not want an IP address returned by the client.
- **Assigned by dialup client**—Select this option to use the IP address dialup client assignment.
- **Assign static IP address**—Select this option and type the IP address in the box, if a specific IP address should be used for this user.

Note If the IP address is being assigned from a pool of IP addresses or by the dialup client, leave the Assign IP address box blank.

Downloaded from www.Manualslib.com manuals search engine

- **Assigned by AAA client pool**—Select this option and type the AAA client IP pool name in the box, if this user is to have the IP address assigned by an IP address pool configured on the AAA client.
- **Assigned from AAA pool**—Select this option and type the applicable pool name in the box, if this user is to have the IP address assigned by an IP address pool configured on the AAA server. Select the AAA server IP pool name from the Available Pools list, and then click —> (right arrow button) to move the name into the Selected Pools list. If there is more than one pool in the Selected Pools list, the users in this group are assigned to the first available pool in the order listed. To move the position of a pool in the list, select the pool name and click **Up** or **Down** until the pool is in the position you want.

Step 3 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Setting Network Access Restrictions for a User

The Network Access Restrictions table in the Advanced Settings area of User Setup enables you to apply NARs in three distinct ways:

- Apply existing shared NARs by name
- Define IP-based access restrictions to permit or deny user access to a specified AAA client or to specified ports on a AAA client when an IP connection has been established
- Define CLI/DNIS-based access restrictions to permit or deny user access based on the CLI/DNIS used

Note You can also use the CLI/DNIS-based access restrictions area to specify other values. For more information, see the "About Network Access Restrictions" section on page 5-6.

Downloaded from www.Manualslib.com manuals search engine

Typically, you define (shared) NARs from within the Shared Components section so that these restrictions can be applied to more than one group or user. For more information, see the "Shared Network Access Restrictions Configuration" section on page 5-7. You must have selected the User-Level Shared Network Access Restriction check box on the Advanced Options page of the Interface Configuration section for this set of options to appear in the Cisco Secure ACS HTML interface.

However, Cisco Secure ACS also enables you to define and apply a NAR for a single user from within the User Setup section. You must have enabled the User-Level Network Access Restriction setting under the Advanced Options page of the Interface Configuration section for single user IP-based filter options and single user CLI/DNIS-based filter options to appear in the Cisco Secure ACS HTML interface.

Note When an authentication request is forwarded by proxy to a Cisco Secure ACS, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

To set NARs for a user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 To apply a previously configured shared NAR to this user, follow these steps:

Note To apply a shared NAR, you must previously have configured it under Network Access Restrictions in the Shared Profile Components section. For more information, see the "Shared Network Access Restrictions Configuration" section on page 5-7.

a. Select the **Only Allow network access when** check box.

Downloaded from www.Manualslib.com manuals search engine

b. To specify whether one or all shared NARs must apply for the user to be permitted access, select one of the following two options, as applicable:

- **All selected NARS result in permit**
- **Any one selected NAR results in permit**

c. Select a shared NAR name in the NARs list, and then click —> (right arrow button) to move the name into the Selected NARs list.

Tip To view the server details of the shared NARs you have selected to apply, you can click either **View IP NAR** or **View CLID/DNIS NAR**, as applicable.

Step 3 To define and apply a NAR, for this particular user, that permits or denies this user access based on IP address, or IP address and port, follow these steps:

Tip You should define most NARs from within the Shared Components section so that they can be applied to more than one group or user. For more information, see the "Shared Network Access Restrictions Configuration" section on page 5-7.

a. In the Network Access Restrictions table, under Per User Defined Network Access Restrictions, select the **Define IP-based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, select one of the following:

- **Permitted Calling/Point of Access Locations**
- **Denied Calling/Point of Access Locations**

Downloaded from www.Manualslib.com manuals search engine

c. Select or enter the information in the following boxes:

- **AAA Client**—Select **All AAA Clients**, or the name of a network device group (NDG), or the name of the individual AAA client, to which to permit or deny access.
- **Port**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports on the selected AAA client.
- **Address**—Type the IP address or addresses to use when performing access restrictions. You can type multiple entries separated by a comma or use the wildcard asterisk (*).

d. Click **enter**.

Result: The specified AAA client, port, and address information appears in the table above the AAA Client list.

Step 4 To permit or deny this user access based on calling location or values other than an established IP address, follow these steps:

a. Select the **Define CLI/DNIS based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, select one of the following:

- **Permitted Calling/Point of Access Locations**
- **Denied Calling/Point of Access Locations**

Downloaded from www.Manualslib.com manuals search engine

c. Complete the following boxes:

Note You must make an entry in each box. You can use the wildcard asterisk (*) for all or part of a value. The format you use must match the format of the string you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

- **AAA Client**—Select **All AAA Clients**, or the name of the NDG, or the name of the individual AAA client, to which to permit or deny access.
- **PORT**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports.
- **CLI**—Type the CLI number to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access based on part of the number.

Tip This is also the selection to use if you want to restrict access based on other values such as a Cisco Aironet client's MAC address. For more information, see the "About Network Access Restrictions" section on page 5-6.

- **DNIS**—Type the DNIS number to which to permit or deny access. Use this to restrict access based on the number into which the user will be dialing. You can use the wildcard asterisk (*) to permit or deny access based on part of the number.

Tip This is also the selection to use if you want to restrict access based on other values such as a Cisco Aironet AP's MAC address. For more information, see the "About Network Access Restrictions" section on page 5-6.

d. Click **enter**.

Result: The information, specifying the AAA client, port, CLI, and DNIS appears in the table above the AAA Client list.

Downloaded from www.Manualslib.com manuals search engine

Step 5 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Setting Max Sessions Options for a User

The Max Sessions feature enables you to set the maximum number of simultaneous connections permitted for this user. For Cisco Secure ACS purposes, a session is considered any type of user connection supported by RADIUS or TACACS+, for example PPP, or Telnet, or ARAP. Note, however, that accounting must be enabled on the AAA client for Cisco Secure ACS to be aware of a session. All session counts are based on user and group names only. Cisco Secure ACS does not support any differentiation by type of session—all sessions are counted as the same. To illustrate, a user with a Max Session count of 1 who is dialed in to a AAA client with a PPP session will be refused a connection if that user then tries to Telnet to a location whose access is controlled by the same ACS.

Note Each Cisco Secure ACS server holds its own Max Sessions counts. There is no mechanism for Cisco Secure ACS to share Max Sessions counts across multiple servers. Therefore, if two Cisco Secure ACS servers are set up as a mirror pair with the workload distributed between them, they will have completely independent views of the Max Sessions totals.

Tip If the Max Sessions table does not appear, click **Interface Configuration**, click **Advanced Options**. Then select the **Max Sessions** check box.

Downloaded from www.Manualslib.com manuals search engine

To set max sessions options for a user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 In the Max Sessions table, under Sessions available to user, select one of the following three options:

- **Unlimited**—Select to allow this user an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
- *n*—Select and then type the maximum number of simultaneous sessions to allow this user.
- **Use group setting**—Select to use the Max Sessions value for the group.

Note The default setting is Use group setting.

Note User Max Sessions settings override the group Max Sessions settings. For example, if the group Sales has a Max Sessions value of only 10, but a user in the group Sales, John, has a User Max Sessions value of Unlimited, John is still allowed an unlimited number of sessions.

Step 3 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Setting User Usage Quotas Options

You can define usage quotas for individual users. You can limit users in one or both of two ways:

- By total duration of sessions for the period selected
- By the total number of sessions for the period selected

For Cisco Secure ACS purposes, a session is considered any type of user connection supported by RADIUS or TACACS+, for example PPP, or Telnet, or ARAP. Note, however, that accounting must be enabled on the AAA client for Cisco Secure ACS to be aware of a session. If you make no selections in the Session Quotas section for an individual user, Cisco Secure ACS applies the session quotas of the group to which the user is assigned.

Note If the User Usage Quotas feature does not appear, click **Interface Configuration** followed by **Advanced Options**. Then select the **Usage Quotas** check box.

Tip The Current Usage table under the User Usage Quotas table on the User Setup Edit page displays usage statistics for the current user. The Current Usage table lists both online time and sessions used by the user, with columns for daily, weekly, monthly, and total usage. The Current Usage table appears only on user accounts that you have previously established; that is, it does not appear during initial user setup.

For a user who has exceeded his quota, Cisco Secure ACS denies him access upon his next attempt to start a session. If a quota is exceeded during a session, Cisco Secure ACS allows the session to continue. If a user's account has been disabled because the user has exceeded usage quotas, the User Setup Edit page displays a message stating that the account has been disabled for this reason.

You can reset the session quota counters on the User Setup page for a user. For more information about resetting usage quota counters, see the "Resetting User Session Quota Counters" section on page 7-55.

To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated only when the user logs off. If the AAA client through which the user is accessing your

Downloaded from www.Manualslib.com manuals search engine

network fails, the quota is not updated. In the case of multiple sessions, such as with ISDN, the quota is not updated until all sessions terminate, which means that a second channel will be accepted even if the first channel has exhausted the user's quota.

To set usage quota options for a user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 In the Usage Quotas table, select **Use these settings**.

Step 3 To define a usage quota based on duration of sessions for a user, follow these steps:

a. Select the **Limit user to** *x* **hours of online time** check box.

b. Type the number of hours to which you want to limit the user in the **Limit user to** *x* **hours of online time** box. Use decimal values to indicate minutes. For example, a value of 10.5 would equal 10 hours and 30 minutes.

c. Select the period for which you want to enforce the time usage quota:

- **per Day**—From 12:01 a.m. until midnight
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month
- **Absolute**—A continuous, open-ended count of hours

Step 4 To define usage quotas based on the number of sessions for a user, follow these steps:

a. Select the **Limit user to** *x* **sessions** check box.

b. Type the number of sessions to which you want to limit the user in the **Limit user to** *x* **sessions** box.

Downloaded from www.Manualslib.com manuals search engine

c. Select the period for which you want to enforce the session usage quota:

- **per Day**—From 12:01 a.m. until midnight
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month
- **Absolute**—A continuous, open-ended count of hours

Setting Options for User Account Disablement

The Account Disable feature defines the circumstances upon which a user's account is disabled.

Note Do not confuse this feature with account expiration due to password aging. Password aging is defined for groups only, not for individual users. Also note that this feature is distinct from the Account Disabled check box. For instructions on how to disable a user account, see the "Disabling a User Account" section on page 7-53.

Note If the user is authenticated with a Windows NT/2000 external user database, this expiration information is in addition to the information in the Windows NT/2000 user account. Changes here do not alter settings configured in Windows NT/2000.

To set options for user account disablement, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Do one of the following:

a. Select the **Never** option to keep the user account always enabled.

Note This is the default setting.

b. Select the **Disable account if** option to disable the account under specific circumstances. Then, specify one or both of the circumstances under the following boxes:

- **Date exceeds**—Select the **Date exceeds:** check box. Then select the month and type the date and year on which to disable the account.

Note The default is 30 days after the user is added.

- **Failed attempts exceed**—Select the **Failed attempts exceed** check box and then type the number of consecutive unsuccessful login attempts to allow before disabling the account.

Note The default is 5.

Step 3 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Assigning a PIX ACL to a User

The Downloadable ACLs feature enables you to assign a PIX Access Control List (ACL) at the user level. You must have established one or more PIX ACLs before attempting to assign one. For instructions on how to configure a downloadable

Downloaded from www.Manualslib.com manuals search engine

PIX ACL using the Shared Profile Components section of the Cisco Secure ACS HTML interface, see the "Adding a Downloadable PIX ACL" section on page 5-3.

Note The Downloadable ACLs table does not appear if it has not been enabled. To enable the Downloadable ACLs table, click **Interface Configuration** followed by **Advanced Options**. Then select the **User-Level Downloadable ACLs** check box.

To assign a downloadable PIX ACL to a user account, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added and edited appears at the top of the page.

Step 2 Under the Downloadable ACLs section, click the **Assign PIX ACL:** check box.

Step 3 Select a PIX ACL from the list.

Step 4 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Advanced User Authentication Settings

This section presents the activities you perform to configure user-level TACACS+ and RADIUS enable parameters.

This section contains the following subsections:

- TACACS+ Settings (User), page 7-24
- Advanced TACACS+ Settings (User), page 7-31
- RADIUS Attributes, page 7-36

Downloaded from www.Manualslib.com manuals search engine

TACACS+ Settings (User)

The TACACS+ Settings section permits you to enable and configure the service/protocol parameters to be applied for the authorization of a user. This section contains the following procedures:

- Configuring TACACS+ Settings for a User, page 7-24
- Configuring a Shell Command Authorization Set for a User, page 7-26
- Configuring a PIX Command Authorization Set for a User, page 7-29
- Configuring the Unknown Service Setting for a User, page 7-31

Configuring TACACS+ Settings for a User

You can use this procedure to configure TACACS+ settings at the user level for the following service/protocols:

- PPP IP
- PPP IPX
- PPP Multilink
- PPP Apple Talk
- PPP VPDN
- PPP LCP
- ARAP
- Shell (exec)
- PIX Shell (pixShell)
- SLIP

You can also enable any *new* TACACS+ services that you may have configured. Because having all service/protocol settings display within the User Setup section would be cumbersome, you choose what settings to hide or display at the user level when you perform configure the interface. For more information about setting up new or existing TACACS+ services in the Cisco Secure ACS HTML interface, see the "Protocol Configuration Options for TACACS+" section on page 3-7.

Downloaded from www.Manualslib.com manuals search engine

For more information about attributes, see Appendix C, "TACACS+ Attribute-Value Pairs," or your AAA client documentation. For information on assigning a PIX ACL, see the "Assigning a PIX ACL to a User" section on page 7-22.

Before You Begin

- For the TACACS+ service/protocol configuration to be displayed, a AAA client must have been configured to use TACACS+ as the security control protocol.
- In the Advanced Options section of Interface Configuration, ensure that the Per-user TACACS+/RADIUS Attributes check box is selected.

To configure TACACS+ settings for a user, follow these steps:

Step 1 Click **Interface Configuration** and then click **TACACS+ (Cisco IOS)**. In the TACACS+ Services table, under the heading User, ensure that the check box is selected for each service/protocol you want to configure.

Step 2 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 3 Scroll down to the TACACS+ Settings table and click the bolded service name check box to enable that protocol; for example (PPP IP).

Step 4 To enable specific parameters within the selected service, select the check box next to a specific parameter and then do one of the following, as applicable:

a. Select the **Enabled** check box.

b. Specify a value in the corresponding attribute box.

To specify ACLs and IP address pools, enter the name of the ACL or pool as defined on the AAA client. Leave the box blank if the default (as defined on the AAA client) should be used. For more information about attributes, see Appendix C, "TACACS+ Attribute-Value Pairs," or your AAA client documentation. For information on assigning a PIX ACL, see the "Assigning a PIX ACL to a User" section on page 7-22.

Tip An ACL is a list of Cisco IOS commands used to restrict access to or from other devices and users on the network.

Downloaded from www.Manualslib.com manuals search engine

Step 5 To employ custom attributes for a particular service, select the **Custom attributes** check box under that service, and then specify the attribute/value in the box below the check box.

Step 6 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Configuring a Shell Command Authorization Set for a User

Use this procedure to specify the shell command authorization set parameters for a user. You can choose one of five basic options:

- **None**—No authorization for shell commands
- **Group**—For this user, the group-level shell command authorization set applies
- **Assign a Shell Command Authorization Set for any network device**—One shell command authorization set is assigned, and it applies all network devices
- **Assign a Shell Command Authorization Set on a per Network Device Group Basis**—Particular shell command authorization sets are to be effective on particular NDGs
- **Per User Command Authorization**—Enables you to permit or deny specific Cisco IOS commands and arguments at the user level

Before You Begin

- Ensure that a AAA client has been configured to use TACACS+ as the security control protocol.
- In the Advanced Options section of Interface Configuration, ensure that the Per-user TACACS+/RADIUS Attributes check box is selected.

Downloaded from www.Manualslib.com manuals search engine

- In the TACACS+ (Cisco) section of Interface Configuration, ensure that the Shell (exec) option is selected in the User column.
- Ensure that you have previously configured one or more shell command authorization sets. For detailed steps, see the "Command Authorization Sets Configuration" section on page 5-14.

To specify shell command authorization set parameters for a user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Scroll down to the TACACS+ Settings table and to the Shell Command Authorization Set feature area within it.

Step 3 To prevent the application of any shell command authorization set, select (or accept the default of) the **None** option.

Step 4 To assign the shell command authorization set at the group level, select the **As Group** option.

Step 5 To assign a particular shell command authorization set to be effective on any configured network device, follow these steps:

a. Select the **Assign a Shell Command Authorization Set for any network device** option.

b. Then, from the list directly below that option, select the shell command authorization set you want applied to this user.

Step 6 To create associations that assign a particular shell command authorization set to be effective on a particular NDG, for each association, follow these steps:

a. Select the **Assign a Shell Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and an associated **Command Set**.

c. Click **Add Association**.

Result: The associated NDG and shell command authorization set appear in the table.

Downloaded from www.Manualslib.com manuals search engine

Step 7 To define the specific Cisco IOS commands and arguments to be permitted or denied for this user, follow these steps:

a. Select the **Per User Command Authorization** option.

b. Under Unmatched Cisco IOS commands, select either **Permit** or **Deny**.

If you select Permit, the user can issue all commands not specifically listed. If you select Deny, the user can issue only those commands listed.

c. To list particular commands to be permitted or denied, select the **Command** check box and then type the name of the command, define its arguments using standard permit or deny syntax, and select whether unlisted arguments are to be permitted or denied.

Warning **This is a powerful, advanced feature and should be completed by an administrator skilled with Cisco IOS commands. Correct syntax is the administrator's responsibility. For information on how Cisco Secure ACS employs pattern matching in command arguments, see the "About Pattern Matching" section on page 5-14.**

Tip To enter several commands, you must click **Submit** after specifying a command. A new command entry box appears below the box you just completed.

Step 8 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Configuring a PIX Command Authorization Set for a User

Use this procedure to specify the PIX command authorization set parameters for a user. There are four basic options:

- **None**—No authorization for PIX commands
- **Group**—For this user, the group-level PIX command authorization set applies
- **Assign a PIX Command Authorization Set for any network device**—One PIX command authorization set is assigned, and it applies to all network devices
- **Assign a PIX Command Authorization Set on a per Network Device Group Basis**—Particular PIX command authorization sets are to be effective on particular NDGs

Before You Begin

- Ensure that a AAA client has been configured to use TACACS+ as the security control protocol.
- In the Advanced Options section of Interface Configuration, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.
- In the TACACS+ (Cisco) section of Interface Configuration, ensure that the **PIX Shell (pixShell)** option is selected in the User column.
- Ensure that you have previously configured one or more PIX command authorization sets. For detailed steps, see the "Command Authorization Sets Configuration" section on page 5-14.

To specify PIX command authorization set parameters for a user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Scroll down to the TACACS+ Settings table and to the PIX Command Authorization Set feature area within it.

Step 3 To prevent the application of any PIX command authorization set, select (or accept the default of) the **None** option.

Downloaded from www.Manualslib.com manuals search engine

Step 4 To assign the PIX command authorization set at the group level, select the **As Group** option.

Step 5 To assign a particular PIX command authorization set to be effective on any configured network device, follow these steps:

a. Select the **Assign a PIX Command Authorization Set for any network device** option.

b. From the list directly below that option, select the PIX command authorization set you want applied to this user.

Step 6 To create associations that assign a particular PIX command authorization set to be effective on a particular NDG, for each association, follow these steps:

a. Select the **Assign a PIX Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and an associated **Command Set**.

c. Click **Add Association**.

Result: The associated NDG and PIX command authorization set appear in the table.

Step 7 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Configuring the Unknown Service Setting for a User

If you want TACACS+ AAA clients to permit unknown services, you can select the Default (Undefined) Services check box under Checking this option will PERMIT all UNKNOWN Services.

To configure the Unknown Service setting for a user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Scroll down to the table under the heading Checking this option will PERMIT all UNKNOWN Services.

Step 3 To allow TACACS+ AAA clients to permit unknown services for this user, select the **Default (Undefined) Services** check box.

Step 4 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Advanced TACACS+ Settings (User)

The information presented in this section applies when you have a AAA client with TACACS+ configured.

Tip If the Advanced TACACS+ Settings (User) table does not appear, click **Interface Configuration**, click **TACACS+ (Cisco IOS)**, and then click **Advanced TACACS+ Features**.

Downloaded from www.Manualslib.com manuals search engine

Details on configuring user options with the Advanced TACACS+ Settings are presented in the following three procedures:

- Setting Enable Privilege Options for a User, page 7-32
- Setting TACACS+ Enable Password Options for a User, page 7-34
- Setting TACACS+ Outbound Password for a User, page 7-35

Setting Enable Privilege Options for a User

You use TACACS+ Enable Control with Exec session to control administrator access. Typically, you use it for router management control. From the following four basic options, you can select and specify the privilege level you want a user to have.

- **Use Group Level Setting**—Sets the privileges for this user as those configured at the group level.
- **No Enable Privilege**—Disallows enable privileges for this user.

Note This is the default setting.

- **Max Privilege for any AAA Client**—Enables you to select from a list the maximum privilege level that will apply to this user on any AAA client on which this user is authorized.
- **Define Max Privilege on a per-Network Device Group Basis**—Enables you to associate maximum privilege levels to this user in one or more NDGs.

Note For information about privilege levels, refer to your AAA client documentation.

Tip You must configure NDGs from within Interface Configuration before you can assign user privilege levels to them.

Downloaded from www.Manualslib.com manuals search engine

To select and specify the privilege level for a user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Under TACACS+ Enable Control in the Advanced TACACS+ Settings table, select one of the four privilege options, as follows:

- Use Group Level Setting
- No Enable Privilege

Note (No Enable Privilege is the default setting; when setting up an new user account, it should already be selected.)

- Max Privilege for Any Access Server
- Define Max Privilege on a per-Network Device Group Basis

Step 3 If you selected Max Privilege for Any Access Server in Step 2, select the appropriate privilege level from the corresponding list.

Step 4 If you selected Define Max Privilege on a per-Network Device Group Basis in Step 2, perform the following steps to define the privilege levels on each NDG, as applicable:

a. From the Device Group list, select a device group.

Note You must have previously configured a device group for it to be listed.

b. From the Privilege list, select a privilege level to associate with the selected device group.

Downloaded from www.Manualslib.com manuals search engine

c. Click **Add Association**.

Result: An entry appears in the table, associating the device group with a particular privilege level.

d. Repeat Steps a through c for each device group you want to associate to this user.

Tip To delete an entry, select the entry and then click **Remove Associate**.

Step 5 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Setting TACACS+ Enable Password Options for a User

When setting the TACACS+ Enable Password Options for a user, you have three options to chose from, as follows:

- Use CiscoSecure PAP password
- Use external database password
- Use separate password

To set the options for the TACACS+ Enable password, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Do one of the following:

a. To use the information configured in the Password Authentication section, select **Use CiscoSecure PAP password**.

Note For information about basic password setup, see the "Adding a Basic User Account" section on page 7-5.

b. To employ an external database password, select **Use external database password**, and then choose from the list the database that authenticates this user's enable password.

Note The list of databases displays only the databases that you have configured. For more information, see the "About External User Databases" section on page 11-4.

c. To employ a separate password, click **Use separate password**, and then type and retype to confirm a control password for this user. This password is used in addition to the regular authentication.

Step 3 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Setting TACACS+ Outbound Password for a User

The TACACS+ outbound password enables a AAA client to authenticate itself to another AAA client via outbound authentication. The outbound authentication can be PAP, CHAP, MS-CHAP, or ARAP, and results in the Cisco Secure ACS password being given out. By default, the user's ASCII/PAP or CHAP/MS-CHAP/ARAP password is used. To prevent compromising inbound passwords, you can configure a separate SENDAUTH password.

Downloaded from www.Manualslib.com manuals search engine

Caution Use an outbound password only if you are familiar with the use of a TACACS+ SendAuth/OutBound password.

To set a TACACS+ outbound password for a user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Type and retype to confirm a TACACS+ outbound password for this user.

Step 3 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

RADIUS Attributes

You can configure user attributes for RADIUS authentication either generally, at the IETF level, or for vendor-specific attributes (VSAs) on a vendor-by-vendor basis. For general attributes, see the "Setting IETF RADIUS Parameters for a User" section on page 7-37. Cisco Secure ACS ships with many popular VSAs already loaded and available to configure and apply. For information about creating additional, custom RADIUS VSAs, see the "User-Defined RADIUS Vendors and VSA Sets" section on page E-27.

To configure the VSA for one of the RADIUS network device vendors supported by Cisco Secure ACS, refer to the appropriate procedure as follows:

- Setting Cisco IOS/PIX RADIUS Parameters for a User, page 7-38
- Setting Ascend RADIUS Parameters for a User, page 7-39
- Setting Cisco VPN 3000 Concentrator RADIUS Parameters for a User, page 7-41

Downloaded from www.Manualslib.com manuals search engine

- Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User, page 7-42
- Setting Microsoft RADIUS Parameters for a User, page 7-44
- Setting Nortel RADIUS Parameters for a User, page 7-45
- Setting Juniper RADIUS Parameters for a User, page 7-47
- Setting BBSM RADIUS Parameters for a User, page 7-48

To configure custom VSAs, see the "Setting Custom RADIUS Attributes for a User" section on page 7-49.

Setting IETF RADIUS Parameters for a User

RADIUS attributes are sent as a profile for the user from Cisco Secure ACS to the requesting AAA client.

These parameters display only if all the following are true:

- A AAA client has been configured to use one of the RADIUS protocols in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level IETF RADIUS attributes have been enabled under RADIUS (IETF) in the Interface Configuration section.

Note To display or hide any of these attributes in the HTML interface, see the "Protocol Configuration Options for RADIUS" section on page 3-10.

Note For a list and explanation of RADIUS attributes, see Appendix D, "RADIUS Attributes," or the documentation for your particular network device using RADIUS.

Note RADIUS (Cisco Aironet) is not an option since there are no Cisco Aironet-specific VSAs. The length of user session timeouts is controlled by IETF RADIUS attribute 27, Session-Timeout.

Downloaded from www.Manualslib.com manuals search engine

To configure IETF RADIUS attribute settings to be applied as an authorization for the current user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 In the IETF RADIUS table, for each attribute that you need to authorize for the current user, select the check box next to the attribute and then further define the authorization for the attribute in the box or boxes next to it, as applicable.

Step 3 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Setting Cisco IOS/PIX RADIUS Parameters for a User

The Cisco IOS RADIUS parameters appear only if all the following are true:

- A AAA client has been configured to use RADIUS (Cisco IOS/PIX) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Cisco IOS/PIX) attributes have been enabled under RADIUS (Cisco IOS/PIX) in the Interface Configuration section.

Cisco IOS RADIUS represents only the Cisco IOS VSAs. You must configure both the IETF RADIUS and Cisco IOS RADIUS attributes.

Downloaded from www.Manualslib.com manuals search engine

To configure and enable Cisco IOS RADIUS attributes to be applied as an authorization for the current user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Before configuring Cisco IOS RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see the "Setting IETF RADIUS Parameters for a User" section on page 7-37.

Step 3 In the Cisco IOS/PIX RADIUS Attributes table, to specify the attributes to be authorized for the user, follow these steps:

a. Select the **[009\001] cisco-av-pair** attribute check box.

b. Type the commands (such as TACACS+ commands) to be packed as a RADIUS VSA.

c. Continue to select and define attributes, as applicable.

Step 4 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Setting Ascend RADIUS Parameters for a User

The Ascend RADIUS parameters appear only if all the following are true:

- A AAA client has been configured to use RADIUS (Ascend) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Ascend) attributes you intend to apply have been enabled under RADIUS (Ascend) in the Interface Configuration section.

Downloaded from www.Manualslib.com manuals search engine

Ascend RADIUS represents only the Ascend proprietary attributes. You must configure both the IETF RADIUS and Ascend RADIUS attributes. Proprietary attributes override IETF attributes.

The default attribute setting displayed for RADIUS is `Ascend-Remote-Addr`.

Note To hide or display Ascend RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Ascend)" section on page 3-14.

To configure and enable Ascend RADIUS attributes to be applied as an authorization for the current user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Before configuring Ascend RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see the "Setting IETF RADIUS Parameters for a User" section on page 7-37.

Step 3 In the Ascend RADIUS Attributes table, to specify the attributes that should be authorized for the user, follow these steps:

a. Select the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix D, "RADIUS Attributes," or your AAA client documentation.

Step 4 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Setting Cisco VPN 3000 Concentrator RADIUS Parameters for a User

The Cisco VPN 3000 Concentrator RADIUS attribute configurations appear only if all the following are true:

- A AAA client has been configured to use RADIUS (Cisco VPN 3000) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Cisco VPN 3000) attributes you intend to employ have been enabled under RADIUS (Cisco VPN 3000) in the Interface Configuration section.

Cisco VPN 3000 Concentrator RADIUS represents only the Cisco VPN 3000 Concentrator VSA. You must configure both the IETF RADIUS and Cisco VPN 3000 Concentrator RADIUS attributes.

Note To hide or display Cisco VPN 3000 Concentrator RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Cisco VPN 3000)" section on page 3-15.

To configure and enable Cisco VPN 3000 Concentrator RADIUS attributes to be applied as an authorization for the current user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Before configuring Cisco VPN 3000 Concentrator RADIUS attributes, be sure your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see the "Setting IETF RADIUS Parameters for a User" section on page 7-37.

Downloaded from www.Manualslib.com manuals search engine

Step 3 In the Cisco VPN 3000 Concentrator Attribute table, to specify the attributes that should be authorized for the user, follow these steps:

a. Select the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix D, "RADIUS Attributes," or your AAA client documentation.

Step 4 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User

The Cisco VPN 5000 Concentrator RADIUS attribute configurations display only if all the following are true:

- A AAA client has been configured to use RADIUS (Cisco VPN 5000) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Cisco VPN 5000) attributes you intend to employ have been enabled under RADIUS (Cisco VPN 5000) in the Interface Configuration section.

Cisco VPN 5000 Concentrator RADIUS represents only the Cisco VPN 5000 Concentrator VSA. You must configure both the IETF RADIUS and Cisco VPN 5000 Concentrator RADIUS attributes.

Note To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Cisco VPN 5000)" section on page 3-16.

Downloaded from www.Manualslib.com manuals search engine

To configure and enable Cisco VPN 5000 Concentrator RADIUS attributes to be applied as an authorization for the current user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Before configuring Cisco VPN 5000 Concentrator RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see the "Setting IETF RADIUS Parameters for a User" section on page 7-37.

Step 3 In the Cisco VPN 5000 Concentrator Attribute table, to specify the attributes that should be authorized for the user, follow these steps:

a. Select the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix D, "RADIUS Attributes," or your AAA client documentation.

Step 4 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Setting Microsoft RADIUS Parameters for a User

Microsoft RADIUS provides VSAs supporting Microsoft Point-to-Point Encryption (MPPE), which is an encryption technology developed by Microsoft to encrypt point-to-point (PPP) links. These PPP connections can be via a dial-in line, or over a Virtual Private Network (VPN) tunnel. The Microsoft RADIUS attribute configurations display only if both the following are true:

- A AAA client has been configured in Network Configuration that uses a RADIUS protocol that supports the Microsoft RADIUS VSA.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- The user-level RADIUS (Microsoft) attributes you intend to employ have been enabled under RADIUS (Microsoft) in the Interface Configuration section.

The following Cisco Secure ACS RADIUS protocols support the Microsoft RADIUS VSA:

- Cisco IOS
- Cisco VPN 3000
- Cisco VPN 5000
- Ascend

Microsoft RADIUS represents only the Microsoft VSA. You must configure both the IETF RADIUS and Microsoft RADIUS attributes.

Note To hide or display Microsoft RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Microsoft)" section on page 3-17.

To configure and enable Microsoft RADIUS attributes to be applied as an authorization for the current user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Before configuring Cisco IOS RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see the "Setting IETF RADIUS Parameters for a User" section on page 7-37.

Step 3 In the Microsoft RADIUS Attributes table, to specify the attributes that should be authorized for the user, follow these steps:

a. Select the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix D, "RADIUS Attributes," or your AAA client documentation.

Note The MS-CHAP-MPPE-Keys attribute value is generated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 4 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Setting Nortel RADIUS Parameters for a User

The Nortel RADIUS parameters appear only if all the following are true:

- A AAA client has been configured to use RADIUS (Nortel) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Nortel) attributes you intend to apply have been enabled under RADIUS (Nortel) in the Interface Configuration section.

Downloaded from www.Manualslib.com manuals search engine

Nortel RADIUS represents only the Nortel proprietary attributes. You must configure both the IETF RADIUS and Nortel RADIUS attributes. Proprietary attributes override IETF attributes.

Note To hide or display Nortel RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Nortel)" section on page 3-18.

To configure and enable Nortel RADIUS attributes to be applied as an authorization for the current user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Before configuring Nortel RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see the "Setting IETF RADIUS Parameters for a User" section on page 7-37.

Step 3 In the Nortel RADIUS Attributes table, to specify the attributes that should be authorized for the user, follow these steps:

a. Select the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix D, "RADIUS Attributes," or your AAA client documentation.

Step 4 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

Setting Juniper RADIUS Parameters for a User

The Juniper RADIUS parameters appear only if all the following are true:

- A AAA client has been configured to use RADIUS (Juniper) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Juniper) attributes you intend to apply have been enabled under RADIUS (Juniper) in the Interface Configuration section.

Juniper RADIUS represents only the Juniper proprietary attributes. You must configure both the IETF RADIUS and Juniper RADIUS attributes. Proprietary attributes override IETF attributes.

Note To hide or display Juniper RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Juniper)" section on page 3-19.

To configure and enable Juniper RADIUS attributes to be applied as an authorization for the current user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Before configuring Juniper RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see the "Setting IETF RADIUS Parameters for a User" section on page 7-37.

Step 3 In the Juniper RADIUS Attributes table, to specify the attributes that should be authorized for the user, follow these steps:

a. Select the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix D, "RADIUS Attributes," or your AAA client documentation.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Setting BBSM RADIUS Parameters for a User

The BBSM RADIUS parameters appear only if all the following are true:

- A AAA client has been configured to use RADIUS (BBSM) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (BBSM) attributes you intend to apply have been enabled under RADIUS (BBSM) in the Interface Configuration section.

BBSM RADIUS represents only the BBSM proprietary attributes. You must configure both the IETF RADIUS and BBSM RADIUS attributes. Proprietary attributes override IETF attributes.

Note To hide or display BBSM RADIUS attributes, see the "Setting Protocol Configuration Options for RADIUS (Cisco BBSM)" section on page 3-20.

To configure and enable BBSM RADIUS attributes to be applied as an authorization for the current user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Before configuring BBSM RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see the "Setting IETF RADIUS Parameters for a User" section on page 7-37.

Downloaded from www.Manualslib.com manuals search engine

Step 3 In the BBSM RADIUS Attributes table, to specify the attributes that should be authorized for the user, follow these steps:

a. Select the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix D, "RADIUS Attributes," or your AAA client documentation.

Step 4 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Setting Custom RADIUS Attributes for a User

Custom RADIUS parameters appear only if all the following are true:

- You have defined and configured the custom RADIUS VSAs. (For information about creating user-defined RADIUS VSAs, see the "User-Defined RADIUS Vendors and VSA Sets" section on page E-27.)
- A AAA client has been configured in Network Configuration that uses a RADIUS protocol that supports the custom VSA.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (*custom name*) attributes you intend to apply have been enabled under RADIUS (*custom name*) in the Interface Configuration section.

You must configure both the IETF RADIUS and the custom RADIUS attributes. Proprietary attributes override IETF attributes.

Downloaded from www.Manualslib.com manuals search engine

To configure and enable custom RADIUS attributes to be applied as an authorization for the current user, follow these steps:

Step 1 Perform Steps 1 through 3 of the "Adding a Basic User Account" section on page 7-5.

Result: The User Setup Edit page opens. The username being added or edited appears at the top of the page.

Step 2 Before configuring custom RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see the "Setting IETF RADIUS Parameters for a User" section on page 7-37.

Step 3 In the RADIUS *custom name* Attributes table, to specify the attributes that should be authorized for the user, follow these steps:

a. Select the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it, as required.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix D, "RADIUS Attributes," or your AAA client documentation.

Step 4 Do one of the following:

a. If you are finished configuring the user account options, click **Submit** to record the options.

b. To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Downloaded from www.Manualslib.com manuals search engine

User Management

This section describes how to use the Cisco Secure ACS User Setup section to perform a variety of user account managerial tasks.

This section contains the following procedures:

- Listing All Users, page 7-51
- Finding a User, page 7-52
- Disabling a User Account, page 7-53
- Deleting a User Account, page 7-54
- Resetting User Session Quota Counters, page 7-55
- Resetting a User Account after Login Failure, page 7-55
- Saving User Settings, page 7-56

Listing All Users

The Cisco Secure ACS User List displays all user accounts (enabled and disabled). The list includes, for each user, the username, status, and the group to which the user belongs.

Usernames are displayed in the order in which they were entered into the database. This list cannot be sorted.

Note You can also generate a report of all users, sorted by groups, by using the command-line utility, CSUtil.exe. For more information, see Appendix E, "Cisco Secure ACS Command-Line Database Utility."

To view a list of all user accounts, follow these steps:

Step 1 In the navigation bar, click **User Setup**.

Result: The User Setup Select page opens.

Step 2 Click **List All Users**.

Result: In the display area on the right, the User List appears.

Downloaded from www.Manualslib.com manuals search engine

Step 3 To view or edit the information for an individual user, click the username in the right window.

Result: The user's account information appears.

Finding a User

To find a user, follow these steps:

Step 1 In the navigation bar, click **User Setup**.

Result: The User Setup Select page opens.

Step 2 Type the name in the **User** box and then click **Find**.

Tip You can use wildcard characters (*) in this box.

Tip To display a list of usernames that begin with a particular letter or number, click the letter or number in the alphanumeric list. A list of users whose names begin with that letter or number opens in the display area on the right.

Result: The username, status (enabled or disabled), and group to which the user belongs appear in the display area on the right.

Step 3 To view or edit the information for the user, click the username in the display area on the right.

Result: The user's account information appears.

Downloaded from www.Manualslib.com manuals search engine

Disabling a User Account

This procedure details how to manually disable a user account in the CiscoSecure user database.

Note To configure the conditions by which a user account will automatically be disabled, see the "Setting Options for User Account Disablement" section on page 7-21.

Note This is not to be confused with account expiration due to password aging. Password aging is defined for groups only, not for individual users.

To disable a user account, follow these steps:

Step 1 In the navigation bar, click **User Setup**.

Result: The User Setup Select page opens.

Step 2 In the **User** box, type the name of the user whose account is to be disabled.

Step 3 Click **Add/Edit**.

Result: The User Setup Edit page opens. The username being edited appears at the top of the page.

Step 4 Select the **Account Disabled** check box.

Step 5 Click **Submit** at the bottom of the page.

Result: The specified user account is disabled.

Downloaded from www.Manualslib.com manuals search engine

Deleting a User Account

Caution If you are authenticating using the Unknown User policy, you must also delete the user account from the external user database. This prevents the username from being automatically re-added to the CiscoSecure user database the next time the user attempts to log in.

To delete a user account, follow these steps:

Step 1 Click **User Setup**.

Result: The User Setup Select page of the HTML interface opens.

Step 2 In the **User** box, type the complete username to be deleted.

Note Alternatively, you can click **List All Users** and then select the user from the list that appears.

Step 3 Click **Add/Edit**.

Step 4 At the bottom of the User Setup page, click **Delete**.

Note The Delete button appears only when you are editing user information, not when you are adding a username.

Result: A popup window appears that asks you to confirm the user deletion.

Step 5 Click **OK**.

Result: The user account is removed from the CiscoSecure user database.

Downloaded from www.Manualslib.com manuals search engine

Resetting User Session Quota Counters

You can reset the session quota counters for a user either before or after the user exceeds a quota.

To reset user usage quota counters, follow these steps:

Step 1 Click **User Setup**.

Result: The Select page of the HTML interface opens.

Step 2 In the User box, type the complete username of the user whose session quota counters you are going to reset.

Note Alternatively, you can click **List All Users** and then select the user from the list that appears.

Step 3 Click **Add/Edit**.

Step 4 In the Session Quotas section, select the **Reset All Counters on submit** check box.

Step 5 Click **Submit** at the bottom of the browser page.

Result: The session quota counters are reset for this user. The User Setup Select page appears.

Resetting a User Account after Login Failure

Perform this procedure when an account is disabled because the failed attempts count has been exceeded during an unsuccessful user attempt to log in.

To reset a user account after login failure, follow these steps:

Step 1 Click **User Setup**.

Result: The User Setup Select page of the HTML interface opens.

Step 2 In the **User** box, type the complete username of the account to be reset.

Downloaded from www.Manualslib.com manuals search engine

Note Alternatively, you can click List All Users and then select the user from the list that appears.

Step 3 Click **Add/Edit**.

Step 4 In the Account Disable table, select the **Reset current failed attempts count on submit** check box, and then click **Submit**.

Result: The Failed attempts since last successful login: counter resets to 0 (zero) and the system re-enables the account.

Note This counter shows the number of unsuccessful login attempts since the last time this user logged in successfully.

Note If the user authenticates with a Windows NT/2000 external user database, this expiration information is in addition to the information in the Windows NT/2000 user account. Changes here do not alter settings configured in Windows NT/2000.

Saving User Settings

After you have completed configuration for a user, be sure to save your work.

To save the configuration for the current user, follow these steps:

Step 1 To save the user account configuration, click **Submit**.

Step 2 To verify that your changes were applied, type the username in the **User** box and click **Add/Edit**, and then review the settings.

Downloaded from www.Manualslib.com manuals search engine

Establishing Cisco Secure ACS System Configuration

This chapter addresses the features found in the System Configuration section of Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS).

It contains the following topics:

- Service Control, page 8-2
- Logging, page 8-3
- Date Format Control, page 8-3
- Password Validation, page 8-4
- CiscoSecure Database Replication, page 8-6
- RDBMS Synchronization, page 8-24
- Cisco Secure ACS Backup, page 8-40
- Cisco Secure ACS System Restore, page 8-45
- Cisco Secure ACS Active Service Management, page 8-48
- IP Pools Server, page 8-52
- IP Pools Address Recovery, page 8-59
- VoIP Accounting Configuration, page 8-60
- Cisco Secure ACS Certificate Setup, page 8-61
- Certification Authority Setup, page 8-70
- Global Authentication Setup, page 8-73

Downloaded from www.Manualslib.com manuals search engine

Service Control

Cisco Secure ACS comprises several Windows NT/2000 services. The Service Control page provides basic status information about the services, enables you to configure the service log files, and to stop or restart the services. For more information about Cisco Secure ACS services, see Appendix H, "Cisco Secure ACS Internal Architecture."

This section contains procedures for the following subjects:

- Determining the Status of Cisco Secure ACS Services, page 8-2
- Stopping, Starting, or Restarting Services, page 8-2

You can also configure Cisco Secure ACS service logs. For more information, see the "Configuring Service Logs" section on page 9-35.

Determining the Status of Cisco Secure ACS Services

You can determine whether Cisco Secure ACS services are running or stopped by accessing the Service Control page.

To determine the status of Cisco Secure ACS services, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Service Control**.

Result: The status of the services appears in the CiscoSecure ACS on *hostname* table, where *hostname* is the name of the Cisco Secure ACS server.

Stopping, Starting, or Restarting Services

You can stop, start, or restart Cisco Secure ACS services as needed. This achieves the same result as starting and stopping Cisco Secure ACS services from within Windows NT/2000 Control panel. This stops, starts, or restarts the Cisco Secure ACS services except for CSAdmin, which is responsible for the HTML interface.

Downloaded from www.Manualslib.com manuals search engine

Note If the CSAdmin service needs to be restarted, you can do so using the Control Panel Services applet; however, it is best to allow Cisco Secure ACS to handle the services because there are dependencies in the order in which the services are started.

To stop, start, or restart Cisco Secure ACS services, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Service Control**.

Result: The status of the services appears in the CiscoSecure ACS on *hostname* table, where *hostname* is the name of the Cisco Secure ACS server.

If the services are running, the Restart and Stop buttons appear at the bottom of the page.

If the services are stopped, the Start button appears at the bottom of the page.

Step 3 Click **Stop**, **Start**, or **Restart**, as applicable.

Result: The status of Cisco Secure ACS services changes to the state appropriate to the button you clicked.

Logging

Cisco Secure ACS generates comma-separated value by default, or ODBC log files if so configured, for the administrative and accounting events for the protocols and options you have enabled. For more information, including configuration steps, see Chapter 9, “Working with Logging and Reports.”

Date Format Control

Cisco Secure ACS allows for one of two possible date formats in its logs, reports, and administrative interface. You can choose either a month/day/year format or a day/month/year format.

Downloaded from www.Manualslib.com manuals search engine

Setting the Date Format

Note If you have reports that were generated before you changed the date format, be sure to move or rename them to avoid conflicts. For example, if you are using the month/day/year format, Cisco Secure ACS assigns the name 2001-07-12.csv to a report generated on July 12, 2001. If you subsequently change to the day/month/year format, on December 7, 2001, Cisco Secure ACS creates a file also named 2001-07-12.csv and overwrites the existing file.

To set the date format, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Date Format Control**.

Result: Cisco Secure ACS displays the Date Format Selection table.

Step 3 Select a date format option.

Step 4 Click **Submit & Restart**.

Result: Cisco Secure ACS restarts its services and implements the date format you selected.

Note For the new date format to be seen in the HTML interface reports, you must restart the connection to the Cisco Secure ACS server. Click the Logoff button (a button with an X) in the upper-right corner of the browser window.

Password Validation

The Password Validation option enables you to configure validation parameters for user passwords. Cisco Secure ACS enforces these rules when an administrator changes a user password in the CiscoSecure user database and when a user attempts to change passwords using the CiscoSecure Authentication Agent applet.

Downloaded from www.Manualslib.com manuals search engine

Note Password validation options apply only to user passwords stored in the CiscoSecure user database. They do not apply to passwords in user records kept in external user databases nor do they apply to enable or admin passwords for Cisco IOS network devices.

Setting Password Validation Options

The password validation options are listed below:

- **Password length between *X* and *Y* characters**—Enforces that password lengths be between the values specified in the *X* and *Y* boxes, inclusive. Cisco Secure ACS supports passwords up to 32 characters in length.
- **Password may not contain the username—**Requires that a user password does not contain the username anywhere within it.
- **Password is different from the previous value—**Requires a user's new password to be different from the previous password.
- **Password must be alphanumeric—**Requires a user password to contain both letters and numbers.

To configure password validation options, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Password Validation**.

Result: The Password Validation Options page appears.

Step 3 In Password length between *X* and *Y* characters, type the *minimum* valid number of characters for a password in the *X* box.

Step 4 In Password length between *X* and *Y* characters, type the *maximum* valid number of characters for a password in the *Y* box.

Step 5 To disallow passwords that contain the username, select the **Password may not contain the username** check box.

Step 6 To require that a user's password must be different than the user's previous password, select the **Password is different from the previous value** check box.

Downloaded from www.Manualslib.com manuals search engine

Step 7 To require that passwords must contain both letters and numbers, select the **Password must be alphanumeric** check box.

Step 8 Click **Submit**.

Result: Cisco Secure ACS restarts its services and implements the password validation settings you specified.

CiscoSecure Database Replication

This section provides information about the CiscoSecure Database Replication feature, including procedures for implementing this feature and configuring the Cisco Secure ACS servers involved. This section contains the following topics:

- About CiscoSecure Database Replication, page 8-6
- Important Implementation Considerations, page 8-10
- Database Replication Versus Database Backup, page 8-11
- Database Replication Logging, page 8-12
- Replication Options, page 8-13
- Implementing Primary and Secondary Replication Setups on Cisco Secure ACS Servers, page 8-16
- Configuring a Secondary Cisco Secure ACS Server, page 8-17
- Replicating Immediately, page 8-18
- Scheduling Replication, page 8-20
- Disabling CiscoSecure Database Replication, page 8-23
- Database Replication Event Error Alert Notification, page 8-23

About CiscoSecure Database Replication

Database replication helps make your AAA environment more fault tolerant. Database replication helps create mirror systems of Cisco Secure ACS servers by duplicating parts of the primary Cisco Secure ACS server setup to one or more secondary Cisco Secure ACS servers. You can configure your AAA clients to use

Downloaded from www.Manualslib.com manuals search engine

these secondary Cisco Secure ACS servers if the primary Cisco Secure ACS server fails or is unreachable. With a secondary Cisco Secure ACS server whose CiscoSecure database is a replica of the primary Cisco Secure ACS server's CiscoSecure database, if the primary Cisco Secure ACS server goes out of service, incoming requests are authenticated without network downtime, provided that your AAA clients are configured to failover to the secondary Cisco Secure ACS server.

Database replication allows you to do the following:

- Select the parts of the primary Cisco Secure ACS servers's configuration to be replicated
- Control the timing of the replication process, including creating schedules
- Export selected configuration items from the primary system
- Securely transport selected configuration data from the primary Cisco Secure ACS server to one or more secondary Cisco Secure ACS servers
- Update the secondary Cisco Secure ACS servers to create matching configurations

With regard to database replication, we make the following distinctions about Cisco Secure ACS servers:

- **Primary Cisco Secure ACS server**—A Cisco Secure ACS server that sends replicated CiscoSecure database components to other Cisco Secure ACS servers.
- **Secondary Cisco Secure ACS server**—A Cisco Secure ACS server that receives replicated CiscoSecure database components from a primary Cisco Secure ACS server. In the HTML interface, these are identified as replication partners.

A Cisco Secure ACS server can be both a primary server and a secondary server, provided that it is not configured to be a secondary server to a Cisco Secure ACS server for which it performs as a primary server. Bidirectional replication, wherein an Cisco Secure ACS server both sends database components to and receives database components from the same remote Cisco Secure ACS server, is not supported.

Downloaded from www.Manualslib.com manuals search engine

Note All Cisco Secure ACS servers involved in replication must run the same release of the Cisco Secure ACS software, including patch level. For example, if the primary Cisco Secure ACS server is running Cisco Secure ACS version 3.0.1, all secondary Cisco Secure ACS servers should be running Cisco Secure ACS version 3.0.1.

Replication Process

The database replication process in this section describes the interaction between a primary Cisco Secure ACS server and a secondary Cisco Secure ACS server. This process occurs between a primary Cisco Secure ACS server and each of its secondary Cisco Secure ACS servers.

The database replication process begins when the primary Cisco Secure ACS server compares the list of database components it is configured to replicate with the list of database components each secondary Cisco Secure ACS server is configured to replicate. The primary Cisco Secure ACS server only replicates those database components that it is configured to send and that the secondary Cisco Secure ACS server is configured to receive. If the secondary Cisco Secure ACS server is not configured to receive any of the components that the primary Cisco Secure ACS server is configured to send, the database replication is aborted.

After the primary Cisco Secure ACS server has determined which components to send to the secondary Cisco Secure ACS server, the replication process continues on the primary Cisco Secure ACS server as follows:

1. The primary Cisco Secure ACS server stops its authentication and creates a copy of the CiscoSecure database components that it is configured to replicate. During this step, if AAA clients are configured properly, those that usually use the primary Cisco Secure ACS server failover to another Cisco Secure ACS server.
2. The primary Cisco Secure ACS server resumes its authentication service. It also compresses and encrypts the copy of its database components for transmission to the secondary Cisco Secure ACS server.
3. The primary Cisco Secure ACS server transmits the compressed, encrypted copy of its database components to the secondary Cisco Secure ACS server. This transmission occurs over a TCP connection, using port 2000. The TCP session uses an encrypted, Cisco-proprietary protocol.

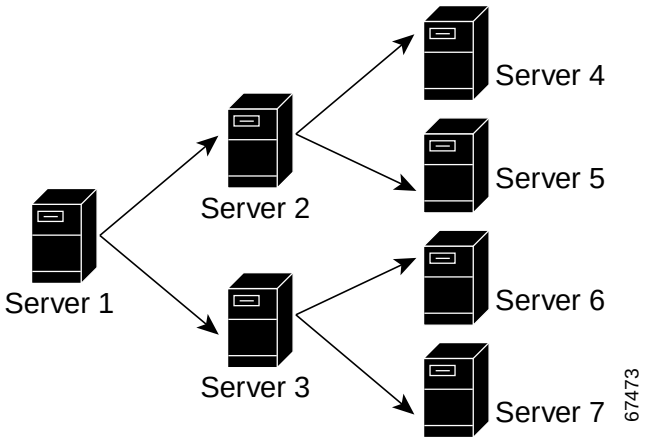
Downloaded from www.Manualslib.com manuals search engine

After the preceding events on the primary Cisco Secure ACS server, the database replication process continues on the secondary Cisco Secure ACS server as follows:

1. The secondary Cisco Secure ACS server receives the compressed, encrypted copy of the primary Cisco Secure ACS server's CiscoSecure database components. After transmission of the database components is complete, the secondary Cisco Secure ACS server uncompresses the database components.
2. The secondary Cisco Secure ACS server stops its authentication service and replaces its database components with the database components it received from the primary Cisco Secure ACS server. During this step, if AAA clients are configured properly, those that usually use the secondary Cisco Secure ACS server failover to another Cisco Secure ACS server.
3. The secondary Cisco Secure ACS server resumes its authentication service.

A Cisco Secure ACS server can act as both a primary server and a secondary server. Figure 8-1 shows a cascading replication scenario. Server 1 acts only as a primary Cisco Secure ACS server, replicating to servers 2 and 3, which act as secondary Cisco Secure ACS servers. After replication from server 1 to server 2 has completed, server 2 acts as a primary Cisco Secure ACS server while replicating to servers 4 and 5. Similarly, server 3 acts as a primary Cisco Secure ACS server while replicating to servers 6 and 7.

Figure 8-1 Cascading Database Replication



Downloaded from www.Manualslib.com manuals search engine

Replication Frequency

The frequency with which your Cisco Secure ACS servers replicate can have important implications for overall AAA performance. With shorter replication frequencies, a secondary server is more up-to-date with the primary server. This allows for a more current secondary Cisco Secure ACS server if the primary Cisco Secure ACS server fails, including a more current CiscoSecure user database.

There is a cost to having frequent replications. The greater the frequency of replication, the higher the load on a multi-server Cisco Secure ACS architecture and your network environment. Because Cisco Secure ACS transfers replicated data more often, network traffic load is much higher. Also, processing load on the synchronizing systems is increased. Replication consumes system resources, and the more often replication is repeated, the greater the impact on the Cisco Secure ACS server's AAA performance.

This issue is more apparent with large databases or frequently changing databases. Database replication is a non-incremental, destructive backup. In other words, it completely replaces the database and configuration on the secondary Cisco Secure ACS server every time it is run. Therefore, if the database being transferred is large, the amount of data being transferred can be substantial, and the processing overhead can also be large.

Important Implementation Considerations

Several important points bear consideration when implementing the CiscoSecure Database Replication feature:

- Cisco Secure ACS only supports database replication to other Cisco Secure ACS servers. All Cisco Secure ACS servers participating in CiscoSecure database replication must run the same version and patch level of Cisco Secure ACS.
- Only suitably configured, valid Cisco Secure ACS hosts can be secondary Cisco Secure ACS servers. To add a secondary Cisco Secure ACS server, configure the Cisco Secure ACS server in the AAA Servers table in the Network Configuration section. When a Cisco Secure ACS server is added to the AAA Servers table, it appears for selection as a secondary Cisco Secure ACS server in the AAA Servers list under Replication Partners on the CiscoSecure Database Replication page.

Downloaded from www.Manualslib.com manuals search engine

- Replication to secondary Cisco Secure ACS servers takes place sequentially in the order listed in the Replication list under Replication Partners on the CiscoSecure Database Replication page.
- The secondary Cisco Secure ACS server receiving the replicated components must be configured to accept database replication from the primary Cisco Secure ACS server. To configure a secondary Cisco Secure ACS server for database replication, see the "Configuring a Secondary Cisco Secure ACS Server" section on page 8-17.
- Cisco Secure ACS does not support bidirectional database replication. The secondary Cisco Secure ACS server receiving the replicated components verifies that the primary Cisco Secure ACS server is not on its Replication list. If not, the secondary Cisco Secure ACS server accepts the replicated components. If so, it rejects the components.
- To replicate user-defined RADIUS vendor and vendor-specific attribute (VSA) configurations successfully, user-defined RADIUS vendor and VSA definitions to be replicated must be identical on the primary and secondary Cisco Secure ACS servers, including the RADIUS vendor slots that the user-defined RADIUS vendors occupy. For more information about user-defined RADIUS vendors and VSAs, see the "User-Defined RADIUS Vendors and VSA Sets" section on page E-27.

Database Replication Versus Database Backup

Do not confuse database replication with system backup. Database replication is *not* a replacement for System Backup. While both features provide protection from partial or complete server loss, each feature addresses the issue in a different way.

System Backup archives data into a format that you can later use to restore the configuration if the system fails or the data becomes corrupted. The backup data is stored on the local hard drive and can be copied and removed from the system for long-term storage. You can store several generations of database backup files.

CiscoSecure Database Replication offers the convenience of copying various components of the CiscoSecure database to other Cisco Secure ACS servers. This can help you plan a failover AAA architecture and can help reduce the complexity of your configuration and maintenance tasks. While it is unlikely, it is possible that CiscoSecure Database Replication can propagate a corrupted database to the Cisco Secure ACS servers that generate your backup files.

Downloaded from www.Manualslib.com manuals search engine

Caution The possibility of backing up a corrupted database exists regardless of whether you use CiscoSecure Database Replication. Because of this small risk, if you are using Cisco Secure ACS in mission-critical environments, we strongly recommend that you implement a backup plan that accounts for this possibility. For more information about backing up the Cisco Secure ACS system or the CiscoSecure database, see the "Cisco Secure ACS Backup" section on page 8-40 and Appendix E, "Cisco Secure ACS Command-Line Database Utility."

Database replication provides fairly comprehensive replication of Cisco Secure ACS servers, but it does not replicate all the Cisco Secure ACS setup. Because Cisco Secure ACS relies on several communication dynamic link libraries (DLLs), database replication does not include external authentication sources. Because the system administrator manually determines which DLLs are installed, database replication cannot rely on the necessary DLLs being present on the replication partners. Use the Cisco Secure ACS System Backup feature to back up these parts of the Cisco Secure ACS configuration.

Database Replication Logging

Regardless of whether replication events are successful or not, Cisco Secure ACS logs all replication events in two files:

- The Windows NT/2000 Event Log
- The Database Replication report

To view the Windows NT/2000 Event Log, use the Windows NT/2000 administration utilities. You can view recent reports in the Reports and Activity section of Cisco Secure ACS.

For more information about Cisco Secure ACS reports, see Chapter 9, "Working with Logging and Reports."

Downloaded from www.Manualslib.com manuals search engine

Replication Options

The Cisco Secure ACS HTML interface provides three sets of options for configuring CiscoSecure Database Replication:

- Replication Components Options, page 8-13
- Replication Scheduling Options, page 8-14
- Replication Partners Options, page 8-15

Replication Components Options

You can specify both the CiscoSecure database components that a Cisco Secure ACS server sends as a primary Cisco Secure ACS server and the components that it receives as a secondary Cisco Secure ACS server. To create a mirror system, all items must be selected.

Note The CiscoSecure database components received by a secondary Cisco Secure ACS server *overwrite* the secondary Cisco Secure ACS server's own CiscoSecure database components. Any information unique to the overwritten database component is lost.

The options that control the components replicated appear in the Replication Components table on the CiscoSecure Database Replication page and are as follows:

- **User and group database—**Replicate the information for groups and users.
- **AAA Servers and AAA Clients tables—**Replicate the AAA Servers tables and the AAA Clients tables in the Network Configuration section.
- **Distribution table—**Replicate the Proxy Distribution Table in the Network Configuration section.
- **Interface configuration—**Replicate the Advanced Options settings from the Interface Configuration section.
- **Interface security settings—**Replicate the security information for the Cisco Secure ACS HTML interface.
- **Password validation settings—**Replicate the password validation settings.

Downloaded from www.Manualslib.com manuals search engine

If mirroring the entire database with a secondary Cisco Secure ACS server might send confidential information, such as the proxy distribution table, you can configure the primary Cisco Secure ACS server to send only a specific category of database information.

Note Cisco Secure ACS does not replicate server certificates used for EAP-TLS authentication. Certificates are unique to a server; therefore, they are excluded from the replication process.

Replication Scheduling Options

You can specify when CiscoSecure database replication occurs. The options that control when replication occurs appear in the Replication Scheduling table on the CiscoSecure Database Replication page and are as follows:

- **Manually—**Cisco Secure ACS does not perform automatic database replication.
- **Automatically Triggered Cascade—**Cisco Secure ACS performs database replication to the configured list of secondary Cisco Secure ACS servers when database replication from a primary Cisco Secure ACS server completes. This enables you to build a propagation hierarchy of Cisco Secure ACS servers, relieving a primary Cisco Secure ACS server from the burden of propagating the replicated components to every other Cisco Secure ACS server. For an illustration of cascade replication, see Figure 8-1 on page 8-9.
- **Every *X* minutes**—Cisco Secure ACS performs, on a set frequency, database replication to the configured list of secondary Cisco Secure ACS servers. The unit of measurement is minutes, with a default update frequency of 60 minutes.
- **At specific times...—**Cisco Secure ACS performs, at the time specified in the day and hour graph, database replication to the configured list of secondary Cisco Secure ACS servers. The minimum resolution is one hour, and the replication takes place on the hour selected.

Downloaded from www.Manualslib.com manuals search engine

Replication Partners Options

You can specify the Cisco Secure ACS servers for which a Cisco Secure ACS performs as a primary Cisco Secure ACS server or as a secondary Cisco Secure ACS server. The options that control the Cisco Secure ACS servers with which a Cisco Secure ACS server is involved for replication appear in the Replication Partners table on the CiscoSecure Database Replication page and are as follows:

- **AAA Server—**This list represents the AAA servers configured in the AAA Servers table in Network Configuration to which a Cisco Secure ACS server *does not* send replicated components.
- **Replication—**This list represents the Cisco Secure ACS servers configured in the AAA Servers table in Network Configuration to which the Cisco Secure ACS server *does* send replicated components. These are Cisco Secure ACS servers for which the Cisco Secure ACS server you are configuring acts as a primary Cisco Secure ACS server.
- **Accept replication from—**The Cisco Secure ACS server selected in this list is the Cisco Secure ACS server from which the current Cisco Secure ACS server does accept replicated components. If Any Known CiscoSecure ACS for Windows 2000/NT Server is selected, the Cisco Secure ACS server accepts replicated components from any Cisco Secure ACS server configured in the AAA Servers table in Network Configuration. This list defines whether this server acts as a secondary Cisco Secure ACS server for a single Cisco Secure ACS server or all Cisco Secure ACS identified in the AAA Servers table.

Note Cisco Secure ACS does not support bidirectional database replication. A secondary Cisco Secure ACS server receiving replicated components verifies that the primary Cisco Secure ACS server is not on its Replication list. If not, the secondary Cisco Secure ACS server accepts the replicated components. If so, it rejects the components.

For more information about the AAA Servers table in Network Configuration, see the "AAA Server Configuration" section on page 4-15.

Downloaded from www.Manualslib.com manuals search engine

Implementing Primary and Secondary Replication Setups on Cisco Secure ACS Servers

If you implement a replication scheme that uses cascading replication, the Cisco Secure ACS server configured to replicate only when it has received replicated components from another Cisco Secure ACS server acts both as a primary Cisco Secure ACS server and as a secondary Cisco Secure ACS server. First, it acts as a secondary Cisco Secure ACS server while it receives replicated components, and then it acts as a primary Cisco Secure ACS while it replicates components to other Cisco Secure ACS servers. For an illustration of cascade replication, see Figure 8-1 on page 8-9.

To implement primary and secondary replication setups on Cisco Secure ACS servers, follow these steps:

Step 1 On each secondary Cisco Secure ACS server, follow these steps:

a. In the Network Configuration section, add the primary Cisco Secure ACS server to the AAA Servers table.

For more information about adding entries to the AAA Servers table, see the "AAA Server Configuration" section on page 4-15.

b. Configure the secondary Cisco Secure ACS server to receive replicated components. For instructions, see the "Configuring a Secondary Cisco Secure ACS Server" section on page 8-17.

Step 2 On the primary Cisco Secure ACS server, follow these steps:

a. In the Network Configuration section, add each secondary Cisco Secure ACS server to the AAA Servers table.

For more information about adding entries to the AAA Servers table, see the "AAA Server Configuration" section on page 4-15.

b. To replicate according to a schedule, at intervals, or whenever the primary Cisco Secure ACS server has received replicated components from another Cisco Secure ACS server, see the "Scheduling Replication" section on page 8-20.

c. To initiate replication immediately, see the "Replicating Immediately" section on page 8-18.

Downloaded from www.Manualslib.com manuals search engine

Configuring a Secondary Cisco Secure ACS Server

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and select the **CiscoSecure ACS Database Replication** check box. Also, verify that the Distributed System Settings check box is selected; if not, select the **Distributed System Settings** check box.

The CiscoSecure Database Replication feature requires that you configure Cisco Secure ACS servers that are to receive replication components, that is, that you configure Cisco Secure ACS servers to act as secondary Cisco Secure ACS servers. The components that a secondary Cisco Secure ACS server is to receive must be explicitly specified, as must be its primary Cisco Secure ACS server or servers.

Replication is always initiated by the primary Cisco Secure ACS server. For more information about sending replication components, see the "Replicating Immediately" section on page 8-18 or the "Scheduling Replication" section on page 8-20.

Caution The CiscoSecure database components received by a secondary Cisco Secure ACS server *overwrite* the secondary Cisco Secure ACS server's own CiscoSecure database components. Any information unique to the overwritten database component is lost.

To configure a Cisco Secure ACS server to be a secondary Cisco Secure ACS server, follow these steps:

Step 1 Log in to the secondary Cisco Secure ACS server's HTML interface.

Step 2 In the navigation bar, click **System Configuration**.

Step 3 Click **CiscoSecure Database Replication**.

Result: The Database Replication Setup page appears.

Step 4 Select the **Receive** check box for each database component to be received from a primary Cisco Secure ACS server.

For more information about replication components, see the "Replication Components Options" section on page 8-13.

Downloaded from www.Manualslib.com manuals search engine

Step 5 If the secondary Cisco Secure ACS server is to receive replication components from *only one* primary Cisco Secure ACS server, from the Accept replication from list, select the other Cisco Secure ACS server name.

Note The primary Cisco Secure ACS servers available in the Accept replication from list is determined by the AAA Servers table in the Network Configuration section. For more information about the AAA Servers table, see the "AAA Server Configuration" section on page 4-15.

Step 6 If the secondary Cisco Secure ACS server is to receive replication components from *more than one* primary Cisco Secure ACS server, from the Accept replication from list, select **Any Known CiscoSecure ACS for Windows 2000/NT Server**.

The Any Known CiscoSecure ACS for Windows 2000/NT Server option is limited to the Cisco Secure ACS servers listed in the AAA Servers table in Network Configuration.

Step 7 Click **Submit**.

Result: Cisco Secure ACS saves the replication configuration, and at the frequency or times you specified, Cisco Secure ACS begins accepting the replicated components from the other Cisco Secure ACS servers you specified.

Replicating Immediately

You can manually start database replication.

Note Replication cannot occur until you have configured at least one secondary Cisco Secure ACS server. For more information about configuring a secondary Cisco Secure ACS server, see the "Configuring a Secondary Cisco Secure ACS Server" section on page 8-17.

Downloaded from www.Manualslib.com manuals search engine

To initiate database replication immediately, follow these steps:

Step 1 Log in to the primary Cisco Secure ACS server's HTML interface.

Step 2 In the navigation bar, click **System Configuration**.

Step 3 Click **CiscoSecure Database Replication**.

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and select the **CiscoSecure ACS Database Replication** check box. Also, verify that the Distributed System Settings check box is selected; if not, select the **Distributed System Settings** check box.

Result: The Database Replication Setup page appears.

Step 4 For each CiscoSecure database component you want to replicate to a secondary Cisco Secure ACS server, under Replication Components, select the corresponding **Send** check box.

Step 5 For each secondary Cisco Secure ACS that you want the primary Cisco Secure ACS server to replicate its select components to, select the secondary Cisco Secure ACS server from the AAA Servers list, and then click —> (right arrow button).

Step 6 To remove secondary Cisco Secure ACS servers from Replication list, select the secondary Cisco Secure ACS server in the Replication list, and then click <— (left arrow button).

Result: The selected secondary Cisco Secure ACS server appears in the AAA Servers list.

Step 7 At the bottom of the browser window, click **Replicate Now**.

Result: Cisco Secure ACS saves the replication configuration. Cisco Secure ACS immediately begins sending replicated database components to the secondary Cisco Secure ACS servers you specified.

Downloaded from www.Manualslib.com manuals search engine

Scheduling Replication

You can schedule when a primary Cisco Secure ACS server sends its replication components to a secondary Cisco Secure ACS server. For more information about replication scheduling options, see the "Configuring a Secondary Cisco Secure ACS Server" section on page 8-17.

Note Replication cannot occur until the secondary Cisco Secure ACS servers are configured properly. For more information about receiving replication components, see the "Configuring a Secondary Cisco Secure ACS Server" section on page 8-17.

To schedule when a primary Cisco Secure ACS server replicates to its secondary Cisco Secure ACS servers, follow these steps:

Step 1 Log in to the primary Cisco Secure ACS server's HTML interface.

Step 2 In the navigation bar, click **System Configuration**.

Step 3 Click **CiscoSecure Database Replication**.

Note If this feature does not appear, click **Interface Configuration**, click Advanced Options, and select the **CiscoSecure ACS Database Replication** check box. Also, verify that the Distributed System Settings check box is selected; if not, select the **Distributed System Settings** check box.

Result: The Database Replication Setup page appears.

Step 4 To specify which CiscoSecure database components the primary Cisco Secure ACS server is to send to its secondary Cisco Secure ACS servers, under Replication Components, select the corresponding **Send** check box for each database component to be sent.

For more information about replication components, see the "Replication Components Options" section on page 8-13.

Downloaded from www.Manualslib.com manuals search engine

Step 5 To have the primary Cisco Secure ACS server send replication components to its secondary Cisco Secure ACS servers at regular intervals, under Replication Scheduling, select the **Every** *X* **minutes** option and in the *X* box type the length of the interval at which Cisco Secure ACS should perform replication.

Note Because Cisco Secure ACS is momentarily shut down during replication, a short replication interval may cause frequent failover of your AAA clients to other Cisco Secure ACS servers. If AAA clients are not properly configured to failover to other Cisco Secure ACS servers, the brief interruption in authentication service may prevent users from authenticating.

Step 6 To schedule times at which the primary Cisco Secure ACS server sends its replication components to its secondary Cisco Secure ACS servers, follow these steps:

a. Under Replication Scheduling, select the **At specific times** option.

b. In the day and hour graph, click the times at which you want Cisco Secure ACS to perform replication.

Tip Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click Clear All to clear all hours, or you can click Set All to select all hours.

Step 7 To have the primary Cisco Secure ACS server send replication components immediately upon receiving replication components from another Cisco Secure ACS server, select the **Automatically triggered cascade** option.

Note If you specify the Automatically triggered cascade option, you must configure another Cisco Secure ACS server to act as a primary Cisco Secure ACS server to this server; otherwise, this Cisco Secure ACS server never replicates to its secondary Cisco Secure ACS servers.

Downloaded from www.Manualslib.com manuals search engine

Step 8 To specify the secondary Cisco Secure ACS servers for the primary Cisco Secure ACS server, follow these steps:

Note For more information about replication partners, see the "Replication Partners Options" section on page 8-15.

a. In the Replication Partners table, from the AAA Servers list, select the name of a secondary Cisco Secure ACS server to which you want the primary Cisco Secure ACS server to send its selected replication components.

Note The secondary Cisco Secure ACS servers available in the AAA Servers list is determined by the AAA Servers table in Network Configuration. For more information about the AAA Servers table, see the "AAA Server Configuration" section on page 4-15.

b. Click —> (right arrow button).

Result: The selected secondary Cisco Secure ACS server moves to the Replication list.

c. Repeat Steps a and b for each secondary Cisco Secure ACS server to which you want the primary Cisco Secure ACS server to send its selected replication components.

d. If you move more than one secondary Cisco Secure ACS server to the Replication list, assign the order in which the primary Cisco Secure ACS replicates to them. Click **Up** and **Down** to move selected Cisco Secure ACS servers in the Replication list until you have created the order you want.

Step 9 Click **Submit**.

Result: Cisco Secure ACS saves the replication configuration you created.

Downloaded from www.Manualslib.com manuals search engine

Disabling CiscoSecure Database Replication

You can disable scheduled CiscoSecure database replications without losing the schedule itself. This allows you to cease scheduled replications temporarily and later resume them without having to re-enter the schedule information.

To disable CiscoSecure database replication, follow these steps:

Step 1 Log in to the primary Cisco Secure ACS server's HTML interface.

Step 2 In the navigation bar, click **System Configuration**.

Step 3 Click **CiscoSecure Database Replication**.

Result: The Database Replication Setup page appears.

Step 4 In the Replication Components table, clear all check boxes.

Step 5 In the Replication Scheduling table, select the **Manually** option.

Step 6 Click **Submit**.

Result: Cisco Secure ACS does not permit any replication to or from this Cisco Secure ACS server.

Database Replication Event Error Alert Notification

If replication fails, Cisco Secure ACS displays an error message in red at the top of the Database Replication page. In addition to error notification, the message also displays the error code generated by the last unsuccessful run and suggests you check the error log messages generated for previous failures. To acknowledge and close the message, click **OK**.

Downloaded from www.Manualslib.com manuals search engine

RDBMS Synchronization

This section provides information about the RDBMS Synchronization feature, including procedures for implementing this feature, both within Cisco Secure ACS and the external data source involved. This section contains the following topics:

- About RDBMS Synchronization, page 8-24
- RDBMS Synchronization Components, page 8-25
- Cisco Secure ACS Database Recovery Using the accountActions Table, page 8-28
- Reports and Event (Error) Handling, page 8-29
- Preparing to Use RDBMS Synchronization, page 8-29
- Considerations for Using CSV-Based Synchronization, page 8-30
- Configuring a System Data Source Name for RDBMS Synchronization, page 8-32
- RDBMS Synchronization Options, page 8-33
- Performing RDBMS Synchronization Immediately, page 8-35
- Scheduling RDBMS Synchronization, page 8-37
- Disabling Scheduled RDBMS Synchronizations, page 8-39

About RDBMS Synchronization

The RDBMS Synchronization feature provides the ability to update the CiscoSecure user database with information from an ODBC-compliant data source. The ODBC-compliant data source can be the RDBMS database of a third-party application. It can also be an intermediate file or database that a third-party system updates. Regardless of where the file or database resides, Cisco Secure ACS reads the file or database via the ODBC connection. You can also regard RDBMS Synchronization as an API—anything you can configure for a user, group, or device through the Cisco Secure ACS HTML interface, you can alternatively maintain through this feature. RDBMS Synchronization supports addition, modification, and deletion for all data items it can access.

Downloaded from www.Manualslib.com manuals search engine

You can configure synchronization to occur on a regular schedule. You can also perform synchronizations manually, updating the CiscoSecure user database on demand.

Synchronization performed by a single Cisco Secure ACS server can update the internal databases of other Cisco Secure ACS servers, so that you only need configure RDBMS Synchronization on one Cisco Secure ACS server. Communication between Cisco Secure ACS servers for the purposes of RDBMS Synchronization occurs using an encrypted, Cisco-proprietary protocol.

RDBMS Synchronization Components

The RDBMS Synchronization feature comprises two components:

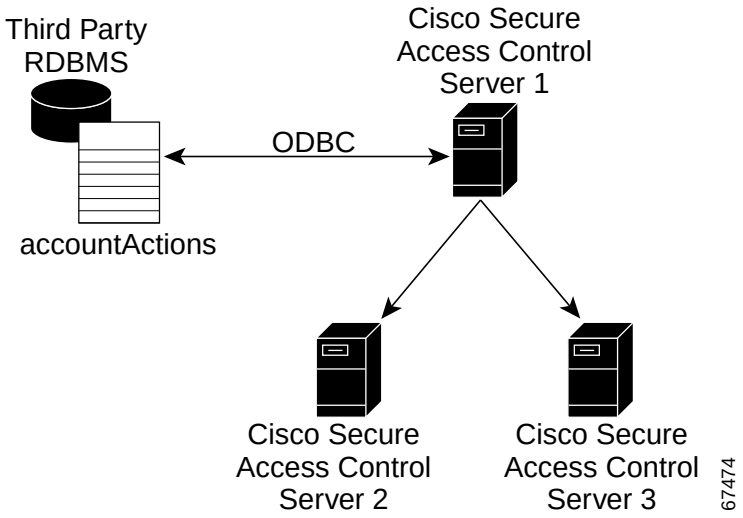
- **CSDBSync—**A dedicated Windows NT/2000 Service that performs automated user and group account management services for Cisco Secure ACS
- **accountActions Table—**The data object that holds information used by CSDBSync to update the CiscoSecure user database

About CSDBSync

The CSDBSync service uses an ODBC system data source name (DSN) to access the accountActions table. See Figure 8-2 on page 8-26. It looks specifically for a table named “accountActions”. Synchronization events fail if CSDBSync cannot access the accountActions table.

Downloaded from www.Manualslib.com manuals search engine

Figure 8-2 RDBMS Synchronization



CSDBSync reads each record from the accountActions table and updates the CiscoSecure user database as specified by the action code in the record. For example, a record could instruct CSDBSync to add a user or a change a user's password. After CSDBSync processes each record, it deletes the record from the table.

CSDBSync both reads and writes (deletes records) in the accountActions table. This requires that the database user account that you configure the system DSN to use must have both read and write privileges.

For more information about CSDBSync or other Windows services used by Cisco Secure ACS, see Appendix H, "Cisco Secure ACS Internal Architecture."

About the accountActions Table

The accountActions table contains a set of rows that define actions CSDBSync is to perform in the CiscoSecure user database. Each row in the accountActions table holds user, user group, or AAA client information. Each row also contains an action field and several other fields. These fields provide CSDBSync with the information it needs to update the CiscoSecure user database. For full details of the accountActions table format and available actions, see Appendix G, "ODBC Import Definitions."

Downloaded from www.Manualslib.com manuals search engine

The database containing the accountActions table must support a multi-threaded ODBC driver. This is required to prevent problems in the event that Cisco Secure ACS and the third-party system attempt to access the accountActions table simultaneously.

Cisco Secure ACS includes files to help you create your accountActions table for several common formats. You can find these files on the Cisco Secure ACS server in the following location, assuming a default installation of Cisco Secure ACS:

`C:\Program Files\CiscoSecure ACS v`*x.x*`\CSDBSync\Databases`

The Databases directory contains the following subdirectories:

- **Access—**Contains the file `CiscoSecure Transactions.mdb`.

  `CiscoSecure Transactions.mdb` contains a preconfigured accountActions table. When you install Cisco Secure ACS, the installation routine creates a system DSN named CiscoSecure DBSync. This system DSN configured to communicate with `CiscoSecure Transactions.mdb`.

Note By default, the username and password for the `CiscoSecure Transactions.mdb` database are set to null. To increase the security of RDBMS synchronizations performed using this database, change the username and password, both in the `CiscoSecure Transactions.mdb` database and in Cisco Secure ACS. Any other processes that access the `CiscoSecure Transactions.mdb` database should be changed to use the new username and password, too.

- **CSV—**Contains the files accountactions and schema.ini.

  The accountactions file is the accountActions table in a comma-separated value file. The schema.ini file provides the Microsoft ODBC text file driver with the information it needs to access the accountactions file.

- **Oracle 7—**Contains the files accountActions.sql and testData.sql.

  The accountActions.sql file contains the Oracle 7 SQL procedure needed to generate an accountActions table. The testData.sql file contains Oracle 7 SQL procedures for updating the accountActions table with sample transactions that CSDBSync can process.

Downloaded from www.Manualslib.com manuals search engine

- **Oracle 8—**Contains the files accountActions.sql and testData.sql.

  The accountActions.sql file contains the Oracle 8 SQL procedure needed to generate an accountActions table. The testData.sql file contains Oracle 8 SQL procedures for updating the accountActions table with sample transactions that CSDBSync can process.

- **SQL Server 6.5—**Contains the files accountActions.sql and testData.sql.

  The accountActions.sql file contains the Microsoft SQL Server 6.5 SQL procedure needed to generate an accountActions table. The testData.sql file contains Microsoft SQL Server 6.5 SQL procedures for updating the accountActions table with sample transactions that CSDBSync can process.

Cisco Secure ACS Database Recovery Using the accountActions Table

Because the RDBMS Synchronization feature deletes each record in the ODBC Import table after processing the record, the accountActions table can be considered a transaction queue. The RDBMS Synchronization feature does not maintain a transaction log/audit trail. If a log is required, the external system that adds records to the accountActions table must create it. Unless the external system can recreate the entire transaction history in the accountActions table, we recommend that you construct a transaction log file for recovery purposes. To do this, create a second table that is stored in a safe location and backed up on a regular basis. In that second table, mirror all the additions and updates to records in the accountActions table.

If the database is large, it is not practical to recreate the CiscoSecure user database by replaying the transaction log for the entire history of the system. Instead, create regular backups of the CiscoSecure user database and replay the transaction logs from the time of most recent backup to bring the CiscoSecure user database back in synchronization with the third-party system. For information on creating backup files, see the "Cisco Secure ACS Backup" section on page 8-40.

Replaying transaction logs that slightly predate the checkpoint does not damage the CiscoSecure user database, although some transactions might be invalid and reported as errors. As long as the entire transaction log is replayed, the CiscoSecure user database is consistent with the external RDBMS application's database.

Downloaded from www.Manualslib.com manuals search engine

Reports and Event (Error) Handling

The CSDBSync service provides event and error logging. For more information about the RDBMS Synchronization log, see the "RDBMS Synchronization Log" section on page 9-16. For more information about the CSDBSync service log, see the "Service Logs" section on page 9-34.

During manual synchronizations, Cisco Secure ACS provides visual alerts to notify you of problems that occurred during synchronization.

Preparing to Use RDBMS Synchronization

Synchronizing the CiscoSecure user database using data from the accountActions table requires that you complete several significant steps external to Cisco Secure ACS before configuring the RDBMS Synchronization feature within Cisco Secure ACS. If you are planning to use a CSV file as your accountActions table, also see the "Considerations for Using CSV-Based Synchronization" section on page 8-30.

To prepare to use RDBMS Synchronization, follow these steps:

Step 1 Determine where you want to create the accountActions table and in what format. For more information about the accountActions table, see the "About the accountActions Table" section on page 8-26. For details on the format and content of the accountActions table, see Appendix G, "ODBC Import Definitions."

Step 2 Create your accountActions table.

Step 3 Configure your third-party system to generate records and update the accountActions table with them. This will most likely involve creating stored procedures that write to the accountActions table at a triggered event; however, the mechanism for maintaining your accountActions table is unique to your implementation. If the third-party system you are using to update the accountActions table is a commercial product, for assistance, refer to the documentation supplied by your third-party system vendor.

For information about the format and content of the accountActions table, see the Appendix G, "ODBC Import Definitions."

Downloaded from www.Manualslib.com manuals search engine

Step 4 Validate your third-party system to ensure that it updates the accountActions table properly. Rows generated in the accountActions table must be valid. For details on the format and content of the accountActions table, see Appendix G, "ODBC Import Definitions."

Note After testing that the third-party system updates the accountActions table properly, discontinue updating the accountActions table until after you have completed Step 5 and Step 6 below.

Step 5 Set up a system DSN on the Cisco Secure ACS server. For steps, see the "Configuring a System Data Source Name for RDBMS Synchronization" section on page 8-32.

Step 6 Schedule RDBMS synchronization in Cisco Secure ACS. For steps, see the "Scheduling RDBMS Synchronization" section on page 8-37.

Step 7 Configure your third-party system to begin updating the accountActions table with information to be imported into the CiscoSecure user database.

Step 8 Confirm that RDBMS synchronization is operating properly by monitoring the RDBMS Synchronization report in the Reports and Activity section. For more information about the RDBMS Synchronization log, see the "RDBMS Synchronization Log" section on page 9-16.

Also, monitor the CSDBSync service log. For more information about the CSDBSync service log, see the "Service Logs" section on page 9-34.

Considerations for Using CSV-Based Synchronization

The behavior of the Microsoft ODBC driver for text files creates significant additional considerations if you are planning to use a CSV-based accountActions table. The Microsoft ODBC driver for text files always operates in a read-only mode. It cannot delete records from a CSV accountActions table. Because of this, synchronization events initiated or scheduled in the HTML interface never release the CSV file, so the updates to the accountActions table from your third-party system fail.

Downloaded from www.Manualslib.com manuals search engine

The solution is to initiate synchronization events from a script, such as a DOS batch file. In the script, RDBMS synchronization is initiated with the **CSDBSync -run** command.

Assuming a default installation, CSDBSync.exe is installed at:

`C:\Program Files\CiscoSecure ACS v`*x.x*`\CSDBSync`

After you have written a script that uses the CSDBsync command, you can schedule synchronization events using the Windows **at** command. For information about the **at** command, please refer to your Microsoft Windows documentation.

Also, due to limitations of the Microsoft ODBC text file driver, using the CSV format requires a change to the accountactions CSV file shipped with Cisco Secure ACS and to Cisco Secure ACS configuration. For more information, see the "Preparing for CSV-Based Synchronization" section on page 8-31.

Preparing for CSV-Based Synchronization

If you want to use a CSV file for your accountActions table, some additional configuration is necessary. This is because the Microsoft ODBC CSV driver cannot access the accountActions table unless the file has a .csv file extension.

To prepare for RDBMS synchronization using a CSV file, follow these steps:

Step 1 Rename the accountactions CSV file installed on your Cisco Secure ACS server to `accountactions.csv`.

Assuming a default installation of Cisco Secure ACS, the accountactions file is at the following location:

`C:\Program Files\CiscoSecure ACS v`*x.x*`\CSDBSync\Databases\CSV`

Step 2 Edit the Windows registry:

a. Access the following key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv`*x.x*`\CSDBSync`

b. Edit the OdbcUpdateTable value from `AccountActions` to `accountactions.csv`.

c. Save your changes to the registry.

Downloaded from www.Manualslib.com manuals search engine

Step 3 At a DOS prompt, follow these steps:

a. Type:

```
net stop CSDBSync
```

and press **Enter**.

b. Type:

```
net start CSDBSync
```

and press **Enter**.

Result: The Microsoft ODBC CSV driver can now access the accountActions CSV file properly.

Configuring a System Data Source Name for RDBMS Synchronization

On the Cisco Secure ACS server, a system DSN must exist for Cisco Secure ACS to access the accountActions table. If you plan to use the `CiscoSecure Transactions.mdb` Microsoft Access database provided with Cisco Secure ACS, you can use the `CiscoSecure DBSync` system DSN rather than creating one.

For more information about the `CiscoSecure Transactions.mdb` file, see the "Preparing to Use RDBMS Synchronization" section on page 8-29.

To create a system DSN for use with RDBMS synchronization, follow these steps:

Step 1 In Windows Control Panel, double-click the ODBC Data Sources icon.

Step 2 In the ODBC Data Source Administrator window, click the **System DSN** tab.

Step 3 Click **Add**.

Step 4 Select the driver you need to use with your new DSN, and then click **Finish**.

Result: A dialog box displays fields requiring information specific to the ODBC driver you selected.

Step 5 In the Data Source Name box, type a descriptive name for the DSN.

Downloaded from www.Manualslib.com manuals search engine

Step 6 Complete the other fields required by the ODBC driver you selected. These fields may include information such as the IP address of the server on which the ODBC-compliant database runs.

Step 7 Click **OK**.

Result: The name you assigned to the DSN appears in the System Data Sources list.

Step 8 Close the ODBC window and Windows Control Panel.

Result: The System DSN to be used by Cisco Secure ACS to access your accountActions table is created on your Cisco Secure ACS server.

RDBMS Synchronization Options

The RDBMS Synchronization Setup page, available from System Configuration, provides control of the following items:

- **RDBMS Setup Options, page 8-34**—Defines how Cisco Secure ACS accesses the accountActions table
- **Synchronization Scheduling Options, page 8-34**—Defines when synchronization occurs
- **Synchronization Partners Options, page 8-35**—Defines which Cisco Secure ACS servers are synchronized with data from the accountActions table

Downloaded from www.Manualslib.com manuals search engine

RDBMS Setup Options

The RDBMS Synchronization feature provides the following RDBMS setup options:

- **Data Source—**Specifies which of all the system DSNs available on the Cisco Secure ACS server is to be used to access the accountActions table
- **Username—**Specifies the username Cisco Secure ACS should use to access the database that contains the accountActions table

Note The database user account specified by the username must have sufficient privileges to read and write to the accountActions table.

- **Password—**Specifies the password Cisco Secure ACS uses to access the database that contains the accountActions table

Synchronization Scheduling Options

The RDBMS Synchronization feature provides the following scheduling options:

- **Manually—**Cisco Secure ACS does not perform automatic RDBMS synchronization.
- **Every *X* minutes**—Cisco Secure ACS performs synchronization on a set frequency. The unit of measurement is minutes, with a default update frequency of 60 minutes.
- **At specific times...—**Cisco Secure ACS performs synchronization at the time specified in the day and hour graph. The minimum resolution is one hour, and the synchronization takes place on the hour selected.

Downloaded from www.Manualslib.com manuals search engine

Synchronization Partners Options

The RDBMS Synchronization feature provides the following synchronization partners options:

- **AAA Server—**This list represents the AAA servers configured in the AAA Servers table in Network Configuration for which the Cisco Secure ACS server *does not* perform RDBMS synchronization.
- **Synchronize—**This list represents the AAA servers configured in the AAA Servers table in Network Configuration for which the Cisco Secure ACS server *does* perform RDBMS synchronization.

For more information about the AAA Servers table in Network Configuration, see the "AAA Server Configuration" section on page 4-15.

Performing RDBMS Synchronization Immediately

You can manually start an RDBMS synchronization event.

To perform manual RDBMS synchronization, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.

Note If this feature does not appear, click **Interface Configuration**, click Advanced Options, and then select the **RDBMS Synchronization** check box.

Result: The RDBMS Synchronization Setup page appears.

Downloaded from www.Manualslib.com manuals search engine

Step 3 To specify options in the RDBMS Setup table, follow these steps:

Note For more information about RDBMS setup, see the "RDBMS Setup Options" section on page 8-34.

a. From the Data Source list, select the system DSN you configured to communicate with the database that contains your accountActions table.

   For more information about configuring a system DSN for use with RDBMS Synchronization, see the "Configuring a System Data Source Name for RDBMS Synchronization" section on page 8-32.

b. In the Username box, type the username for a database user account that has read/write access to the accountActions table.

c. In the Password box, type the password for the username specified in the previous step.

Result: Cisco Secure ACS has the information necessary to access the accountActions table.

Note It is *not* necessary to select Manually under Replication Scheduling. For more information, see the "Disabling Scheduled RDBMS Synchronizations" section on page 8-39.

Step 4 For each Cisco Secure ACS that you want this Cisco Secure ACS server to update with data from the accountActions table, select the Cisco Secure ACS server in the AAA Servers list, and then click —> (right arrow button).

Result: The selected Cisco Secure ACS server appears in the Synchronize list.

Step 5 To remove Cisco Secure ACS servers from Synchronize list, select the Cisco Secure ACS server in the Synchronize list, and then click <— (left arrow button).

Result: The selected Cisco Secure ACS server appears in the AAA Servers list.

Downloaded from www.Manualslib.com manuals search engine

Step 6 At the bottom of the browser window, click **Synchronize Now**.

Result: Cisco Secure ACS immediately begins a synchronization event. To check on the status of the synchronization, view the RDBMS Synchronization report in Reports and Activity.

Scheduling RDBMS Synchronization

You can schedule when a Cisco Secure ACS server performs RDBMS synchronization.

To schedule when a Cisco Secure ACS server performs RDBMS synchronization, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **RDBMS Synchronization** check box.

Result: The RDBMS Synchronization Setup page appears.

Step 3 To specify options in the RDBMS Setup table, follow these steps:

Note For more information about RDBMS setup, see the "RDBMS Setup Options" section on page 8-34.

a. From the Data Source list, select the system DSN you configured to communicate with the database that contains your accountActions table.

For more information about configuring a system DSN for use with RDBMS Synchronization, see the "Configuring a System Data Source Name for RDBMS Synchronization" section on page 8-32.

Downloaded from www.Manualslib.com manuals search engine

b. In the Username box, type the username for a database user account that has read/write access to the accountActions table.

c. In the Password box, type the password for the username specified in the previous step.

Step 4 To have this Cisco Secure ACS server perform RDBMS synchronization at regular intervals, under Synchronization Scheduling, select the **Every** *X* **minutes** option and in the *X* box type the length of the interval at which Cisco Secure ACS should perform synchronization.

Step 5 To schedule times at which this Cisco Secure ACS server performs RDBMS synchronization, follow these steps:

a. Under Synchronization Scheduling, select the **At specific times** option.

b. In the day and hour graph, click the times at which you want Cisco Secure ACS to perform replication.

Tip Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

Step 6 For each Cisco Secure ACS server you want to synchronize with data from the accountActions table, follow these steps:

Note For more information about synchronization targets, see the "Replication Partners Options" section on page 8-15.

a. In the Synchronization Partners table, from the AAA Servers list, select the name of a Cisco Secure ACS server that you want this Cisco Secure ACS server to update with data from the accountActions table.

Note The Cisco Secure ACS servers available in the AAA Servers list is determined by the AAA Servers table in Network Configuration, with the addition of the name of the current Cisco Secure ACS server. For more information about the AAA Servers table, see the "AAA Server Configuration" section on page 4-15.

Downloaded from www.Manualslib.com manuals search engine

b. Click —> (right arrow button).

Result: The selected Cisco Secure ACS server moves to the Synchronize list.

Note At least one Cisco Secure ACS server must be in the Synchronize list. This includes the server on which you are configuring RDBMS Synchronization. RDBMS Synchronization does not automatically include the current server's internal database.

Step 7 Click **Submit**.

Result: Cisco Secure ACS saves the RDBMS synchronization schedule you created.

Disabling Scheduled RDBMS Synchronizations

You can disable scheduled RDBMS synchronization events without losing the schedule itself. This allows you to cease scheduled synchronizations temporarily and later resume them without having to re-enter the schedule information.

To disable scheduled RDBMS synchronizations, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.

Result: The RDBMS Synchronization Setup page appears.

Step 3 Under Synchronization Scheduling, select the **Manually** option.

Step 4 Click **Submit**.

Result: Cisco Secure ACS does not perform scheduled RDBMS synchronizations.

Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS Backup

This section provides information about the Cisco Secure ACS Backup feature, including procedures for implementing this feature. This section contains the following topics:

- About Cisco Secure ACS Backup, page 8-40
- Backup File Locations, page 8-41
- Directory Management, page 8-41
- Components Backed Up, page 8-41
- Reports of Cisco Secure ACS Backups, page 8-42
- Performing a Manual Cisco Secure ACS Backup, page 8-42
- Scheduling Cisco Secure ACS Backups, page 8-43
- Disabling Scheduled Cisco Secure ACS Backups, page 8-44

About Cisco Secure ACS Backup

The ACS Backup process backs up your Cisco Secure ACS system information to a file on the local hard drive. You can manually back up the Cisco Secure ACS system. You can also establish automated backups that occur at regular intervals or at selected days of the week and times. Maintaining backup files can minimize downtime if system information becomes corrupt or is misconfigured. We recommend copying the files to another system's hard drive in case the hardware fails on the primary system.

For information about using a backup file to restore Cisco Secure ACS, see the "Cisco Secure ACS System Restore" section on page 8-45.

Downloaded from www.Manualslib.com manuals search engine

Backup File Locations

The default directory for backup files is the following:

drive:*path*\CSAuth\System Backups

where *drive* is the local drive where you installed Cisco Secure ACS and *path* is the path from the root of *drive* to the Cisco Secure ACS directory. For example, if you installed Cisco Secure ACS Version 3.0 in the default location, the default backup location would be:

```
c:\Program Files\CiscoSecure ACS v3.0\CSAuth\System Backups
```

The filename given to a backup is determined by Cisco Secure ACS. For more information about filenames assigned to backup files generated by Cisco Secure ACS, see the "Backup File Names and Locations" section on page 8-45.

Directory Management

You can configure the number of backup files to keep and the number of days after which backup files are deleted. The more complex your configuration and the more often you back up the system, the more diligent we recommend you be about clearing out old databases from the Cisco Secure ACS server hard drive.

Components Backed Up

The ACS System Backup utility backs up the Cisco Secure ACS user database and information from the Windows Registry that is relevant to Cisco Secure ACS. The user database backup includes all user information, such as username, password, and other authentication information, including server certificates and the certificate trust list. The Windows Registry information includes any system information that is stored in the Windows Registry, such as NDG information, AAA client configuration, and administrator accounts.

Downloaded from www.Manualslib.com manuals search engine

Reports of Cisco Secure ACS Backups

When a system backup takes place, whether it was manually generated or scheduled, the event is logged in the Administration Audit report and the ACS Backup and Restore report. You can view recent reports in the Reports and Activity section of Cisco Secure ACS.

For more information about Cisco Secure ACS reports, see Chapter 9, "Working with Logging and Reports."

Performing a Manual Cisco Secure ACS Backup

You can backup Cisco Secure ACS whenever you want, without scheduling the backup.

To perform an immediate backup of Cisco Secure ACS, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Backup**.

Result: The ACS System Backup Setup page appears.

Step 3 In the Directory box under Backup Location, type the drive and path to the directory on a local hard drive where you want the backup file to be written.

Step 4 Click **Backup Now**.

Result: Cisco Secure ACS immediately begins a backup.

Downloaded from www.Manualslib.com manuals search engine

Scheduling Cisco Secure ACS Backups

You can schedule Cisco Secure ACS backups to occur at regular intervals or at selected days of the week and times.

To schedule the times at which Cisco Secure ACS performs a backup, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Backup**.

Result: The ACS System Backup Setup page appears.

Step 3 To schedule backups at regular intervals, under ACS Backup Scheduling, select the **Every** *X* **minutes** option and in the *X* box type the length of the interval at which Cisco Secure ACS should perform backups.

Note Because Cisco Secure ACS is momentarily shut down during backup, if the backup interval is set too low, users might be unable to authenticate.

Step 4 To schedule backups at specific times, follow these steps:

a. Under ACS Backup Scheduling, select the **At specific times** option.

b. In the day and hour graph, click the times at which you want Cisco Secure ACS to perform a backup.

Tip Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

Step 5 To change the location where Cisco Secure ACS writes backup files, type the drive letter and path in the Directory box.

Downloaded from www.Manualslib.com manuals search engine

Step 6 To manage which backup files Cisco Secure ACS keeps, follow these steps:

a. Select the **Manage Directory** check box.

b. To limit the number of backup files Cisco Secure ACS retains, select the **Keep only the last *X* files** option and type the number of files you want Cisco Secure ACS to retain in the *X* box.

c. To limit how old backup files retained by Cisco Secure ACS can be, select the **Delete files older than *X* days** option and type the number of days for which Cisco Secure ACS should retain a backup file before deleting it.

Step 7 Click **Submit**.

Result: Cisco Secure ACS implements the backup schedule you configured.

Disabling Scheduled Cisco Secure ACS Backups

You can disable scheduled Cisco Secure ACS backups without losing the schedule itself. This allows you to cease scheduled backups temporarily and later resume them without having to re-enter the schedule information.

To disable a scheduled backup, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Backup**.

Result: The ACS System Backup Setup page appears.

Step 3 Under ACS Backup Scheduling, select the **Manual** option.

Step 4 Click **Submit**.

Result: Cisco Secure ACS does not continue any scheduled backups. You can still perform manual backups as needed.

Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS System Restore

This section provides information about the Cisco Secure ACS System Restore feature, including procedures for restoring your Cisco Secure ACS server from a backup file. This section contains the following topics:

- About Cisco Secure ACS System Restore, page 8-45
- Backup File Names and Locations, page 8-45
- Components Restored, page 8-47
- Reports of Cisco Secure ACS Restorations, page 8-47
- Restoring Cisco Secure ACS from a Backup File, page 8-47

About Cisco Secure ACS System Restore

The ACS System Restore feature enables you to restore your system configuration from backup files generated by the ACS Backup feature. This feature helps minimize downtime if Cisco Secure ACS system information becomes corrupted or is misconfigured.

The ACS System Restore feature only works with backup files generated by a Cisco Secure ACS server running an identical release of Cisco Secure ACS, including patch level.

Backup File Names and Locations

The ACS System Restore feature restores the Cisco Secure ACS user database and Cisco Secure ACS Windows Registry information from a file that was created by the ACS Backup feature. Cisco Secure ACS writes backup files only on the local hard drive. You can restore from any backup file you select. For example, you can restore from the latest backup file, or if you suspect that the latest backup was incorrect, you can select an earlier backup file to restore from.

Downloaded from www.Manualslib.com manuals search engine

The backup directory is selected when you schedule backups or perform a manual backup. The default directory for backup files is the following:

drive:*path*\CSAuth\System Backups

where *drive* is the local drive where you installed Cisco Secure ACS and *path* is the path from the root of *drive* to the Cisco Secure ACS directory. For example, if you installed Cisco Secure ACS Version 3.0 in the default location, the default backup location would be:

```
c:\Program Files\CiscoSecure ACS v3.0\CSAuth\System Backups
```

Cisco Secure ACS creates backup files using the date and time format:

dd-mmm-yyyy hh-nn-ss.dmp

where:

- *dd* is the date the backup started
- *mmm* is the month, abbreviated in alphabetic characters
- *yyyy* is the year
- *hh* is the hour, in 24-hour format
- *nn* is the minute
- *ss* is the second at which the backup started

For example, if Cisco Secure ACS started a backup on October 13, 1999, 11:41:35 a.m., Cisco Secure ACS would generate a backup file named:

```
13-Oct-1999 11-41-35.dmp
```

If you are not sure of the location of the latest backup file, check your scheduled backup configuration on the ACS Backup page.

Downloaded from www.Manualslib.com manuals search engine

Components Restored

You can select the components to restore: the user and group databases, the system configuration, or both.

Reports of Cisco Secure ACS Restorations

When a Cisco Secure ACS system restoration takes place, the event is logged in the Administration Audit report and the ACS Backup and Restore report. You can view recent reports in the Reports and Activity section of Cisco Secure ACS.

For more information about Cisco Secure ACS reports, see Chapter 9, "Working with Logging and Reports."

Restoring Cisco Secure ACS from a Backup File

You can perform a system restoration of Cisco Secure ACS whenever needed.

Note Using the Cisco Secure ACS System Restore feature restarts all Cisco Secure ACS services and logs out all administrators.

To restore Cisco Secure ACS from a backup file generated by the Cisco Secure ACS Backup feature, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Restore**.

Result: The ACS System Restore Setup page appears.

The Directory box displays the drive and path to the backup directory most recently configured in the Directory box on the ACS Backup page.

Beneath the Directory box, Cisco Secure ACS displays the backup files in the current backup directory. If no backup files exist, `<No Matching Files>` appears in place of file names.

Downloaded from www.Manualslib.com manuals search engine

Step 3 To change the backup directory, type the new drive and path to the backup directory in the Directory box, and then click **OK**.

Result: Cisco Secure ACS displays the backup files, if any, in the backup directory you specified.

Step 4 In the list below the Directory box, select the backup file you want to use to restore Cisco Secure ACS.

Step 5 To restore user and group database information, select the **User and Group Database** check box.

Step 6 To restore system configuration information, select the **CiscoSecure ACS System Configuration** check box.

Step 7 Click **Restore Now**.

Result: Cisco Secure ACS displays a confirmation dialog box indicating that performing the restoration will restart Cisco Secure ACS services and log out all administrators.

Step 8 To continue with the restoration, click **OK**.

Result: Cisco Secure ACS restores the system components specified using the backup file you selected. The restoration should require several minutes to complete, depending on which components you selected to restore and the size of your database.

When the restoration is complete, you can log in again to Cisco Secure ACS.

Cisco Secure ACS Active Service Management

ACS Active Service Management is an application-specific service monitoring tool that is tightly integrated with ACS. The ACS Active Service Management comprises two features:

- System Monitoring, page 8-49
- Event Logging, page 8-51

Downloaded from www.Manualslib.com manuals search engine

System Monitoring

Cisco Secure ACS system monitoring enables you to determine how often Cisco Secure ACS tests its authentication and accounting processes, and what automated actions it takes should tests detect a failure of these processes.

System Monitoring Options

You have the following options for configuring system monitoring:

- **Test login process every** *X* **minutes**—Controls whether or not Cisco Secure ACS tests its login process. The value in the X box defines, in minutes, how often Cisco Secure ACS tests its login process.

  When this option is enabled, at the interval defined, Cisco Secure ACS tests authentication and accounting. If Cisco Secure ACS detects a failure, it restarts the failed service and retests authentication and accounting. If the second test fails, Cisco Secure ACS performs the action identified in the on failure list. If, after the failure action is performed, testing still fails, Cisco Secure ACS performs event logging. For more information about event logging, see the "Setting Up Event Logging" section on page 8-51.

- **on failure**—Specifies what action Cisco Secure ACS takes if it detects that its login process failed. This list contains several built-in actions and reflects custom actions that you define. The items beginning with asterisks (*) are built-in actions.

  – ***Restart All—**Restart all Cisco Secure ACS services.

  – ***Restart RADIUS/TACACS+—**Restart only the RADIUS and TACACS+ services.

  – ***Reboot**—Reboot the Cisco Secure ACS server.

Downloaded from www.Manualslib.com manuals search engine

  - **Custom actions**—You can define other actions for Cisco Secure ACS to take upon failure of the login process. Cisco Secure ACS can execute a batch file or executable upon the failure of the login process. To make a batch or executable file available in the on failure list, place the file in the following directory:

    drive:*path*\CSMon\Scripts

    where *drive* is the local drive where you installed Cisco Secure ACS and *path* is the path from the root of *drive* to the Cisco Secure ACS directory.
  - **Take No Action—**Leave Cisco Secure ACS operating as is.
- **Generate event when an attempt is made to log in to a disabled account**—Specifies whether or not Cisco Secure ACS generates a Windows event when a user attempts to login to your network using a disabled account.

Setting Up System Monitoring

To setup Cisco Secure ACS System Monitoring, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Service Management**.

Result: The ACS Active Service Management Setup page appears.

Step 3 To have Cisco Secure ACS test the login process, follow these steps:

a. Select the **Test login process every** *X* **minutes** check box.

b. Type the number of minutes that should pass between each login process test in the *X* box.

c. From the on failure list, select the action Cisco Secure ACS should take when the login test fails.

Step 4 To have Cisco Secure ACS generate a Windows event when a user attempts to login to your network using a disabled account, select the **Generate event when an attempt is made to log in to a disabled account** check box.

Downloaded from www.Manualslib.com manuals search engine

Step 5 If you want to setup event logging, proceed to the "Setting Up Event Logging" section on page 8-51.

Step 6 If you are done setting up Cisco Secure ACS Service Management, click **Submit**.

Result: Cisco Secure ACS implements the service management settings you made.

Event Logging

The Event Logging feature enables you to configure whether Cisco Secure ACS logs events to the Windows event log and whether Cisco Secure ACS generates an e-mail when an event occurs. Cisco Secure ACS detects events using the System Monitoring feature. For more information about system monitoring, see the "System Monitoring Options" section on page 8-49.

Setting Up Event Logging

To view the Windows NT/2000 event log, choose **Start** > **Administrative Tools** > **Event Viewer**. For more information about the Windows event log or Event Viewer, refer to your Microsoft Windows documentation.

To setup Cisco Secure ACS event logging, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Service Management**.

Result: The ACS Active Service Management Setup page appears.

Step 3 To have Cisco Secure ACS send all events to the Windows event log, select Log all events to the NT Event log.

Downloaded from www.Manualslib.com manuals search engine

Step 4 To have Cisco Secure ACS send an e-mail when an event occurs, follow these steps:

a. Select the **Email notification of event** check box.

b. In the To box, type the e-mail address to which Cisco Secure ACS should send event notification e-mail.

Note Do not use underscores in the e-mail addresses you type in this box.

c. In the SMTP Mail Server box, type the hostname of the sending email server.

Note The SMTP mail server must be operational and must be available from the Cisco Secure ACS server.

Step 5 If you want to setup system monitoring, proceed to the "Setting Up System Monitoring" section on page 8-50.

Step 6 If you are done setting up Cisco Secure ACS Service Management, click **Submit**.

Result: Cisco Secure ACS implements the service management settings you made.

IP Pools Server

The IP Pools Server feature enables you to assign the same IP address to multiple users, provided that the users are on different segments of the network. This means you can re-use IP addresses and reduce the number of IP addresses on your network. When you enable this feature, Cisco Secure ACS dynamically issues IP addresses from the IP pools you have defined by number or name. You can configure up to 999 IP pools, for approximately 255,000 users.

If you are using IP pooling and proxy, all accounting packets are proxied so that the Cisco Secure ACS that is assigning the IP addresses can confirm whether an IP address is already in use.

Downloaded from www.Manualslib.com manuals search engine

To use IP pools, the AAA client must have network authorization (`aaa authorization network`) and accounting (`aaa accounting`) enabled.

Note To use the IP Pools feature, you must set up your AAA client to perform authentication and accounting using the same protocol—either TACACS+ or RADIUS.

For information on assigning a group or user to an IP pool, see the "Setting IP Address Assignment Method for a User Group" section on page 6-26 or the "Assigning a User to a Client IP Address" section on page 7-11.

Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges

Cisco Secure ACS provides automated detection of overlapping pools.

Note To use overlapping pools, you must be using RADIUS with virtual private networking, and you cannot be using Dynamic Host Configuration Protocol (DHCP).

You can determine whether overlapping IP pools are currently allowed by checking which button appears below the AAA Server IP Pools table:

- **Allow Overlapping Pool Address Ranges—**Indicates that overlapping IP pool address ranges are currently *not allowed*. Clicking the button allows IP address ranges to overlap between pools.
- **Force Unique Pool Address Range—**Indicates that overlapping IP pool address ranges are currently *allowed*. Clicking the button prevents IP address ranges from overlapping between pools.

Downloaded from www.Manualslib.com manuals search engine

To allow overlapping IP pools or to force unique pool address ranges, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **IP Pools** check box.

Result: The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 If you want to allow overlapping IP pool address ranges, follow these steps:

a. If the Allow Overlapping Pool Address Ranges button appears, click that button.

Result: Cisco Secure ACS allows overlapping IP pool address ranges.

b. If the Force Unique Pool Address Range button appears, do nothing.

Cisco Secure ACS already allows overlapping IP pool address ranges.

Step 4 If you want to deny overlapping IP pool address ranges, follow these steps:

a. If the Allow Overlapping Pool Address Ranges button appears, do nothing.

Cisco Secure ACS already does not permit overlapping IP pool address ranges.

b. If the Force Unique Pool Address Range button appears, click that button.

Result: Cisco Secure ACS does not permit overlapping IP pool address ranges.

Downloaded from www.Manualslib.com manuals search engine

Refreshing the AAA Server IP Pools Table

You can refresh the AAA Server IP Pools table. This allows you to get the latest usage statistics for your IP pools.

To refresh the AAA Server IP Pools table, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

Result: The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 Click **Refresh**.

Result: Cisco Secure ACS updates the percentages of pooled addresses in use.

Adding a New IP Pool

You can define up to 999 IP address pools.

To add an IP pool, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

Result: The AAA Server IP Pools table lists any IP pools you have already configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 Click **Add Entry**.

Result: The New Pool table appears.

Step 4 In the Name box, type the name you want to assign to the new IP pool.

Downloaded from www.Manualslib.com manuals search engine

Step 5 In the Start Address box, type the lowest IP address of the range of addresses for the new pool.

Note All addresses in an IP pool must be on the same Class C network, so the first three octets of the start and end addresses must be the same. For example, if the start address is 192.168.1.1, the end address must be between 192.168.1.2 and 192.168.1.254.

Step 6 In the End Address box, type the highest IP address of range of addresses for the new pool.

Step 7 Click **Submit**.

Result: The new IP pool appears in the AAA Server IP Pools table.

Editing an IP Pool Definition

To edit an IP pool definition, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

Result: The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 Click the name of the IP pool you need to edit.

Result: The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use field displays the number of IP addresses of this pool that are currently allocated to a user. The Available field displays the number of IP addresses currently unallocated to users.

Step 4 To change the name of the pool, in the Name box, type the name to which you want to change the IP pool.

Downloaded from www.Manualslib.com manuals search engine

Step 5 To change the starting address of the pool range of IP addresses, in the Start Address box, type the lowest IP address of the new range of addresses for the pool.

Note All addresses in an IP pool must be on the same Class C network, so the first three octets of the start and end addresses must be the same. For example, if the start address is 192.168.1.1, the end address must be between 192.168.1.2 and 192.168.1.254.

Step 6 To change the ending address of the pool range of IP addresses, in the End Address box, type the highest IP address of the new range of addresses for the pool.

Step 7 Click **Submit**.

Result: The edited IP pool appears in the AAA Server IP Pools table.

Resetting an IP Pool

The Reset function recovers IP addresses within an IP pool when there are "dangling" connections. A dangling connection results from a user disconnecting without Cisco Secure ACS receiving an accounting stop packet. If the Failed Attempts log in Reports and Activity shows a large number of "Failed to Allocate IP Address For User" messages, consider using the Reset function to reclaim all allocated addresses in this IP pool.

Note Using the Reset function to reclaim all allocated IP addresses in a pool can result in users being assigned addresses that are already in use.

To reset an IP pool and reclaim all its IP addresses, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

Result: The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Click the name of the IP pool you need to reset.

Result: The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use field displays the number of IP addresses of this pool that are currently assigned to a user. The Available field displays the number of IP addresses currently not assigned to users.

Step 4 Click **Reset**.

Result: Cisco Secure ACS displays a dialog box indicating the possibility of assigning users addresses that are already in use.

Step 5 To continue resetting the IP pool, click **OK**.

Result: The IP pool is reset. All its IP addresses are reclaimed. In the In Use column of the AAA Server IP Pools table, zero percent of the IP pool's addresses are assigned to users.

Deleting an IP Pool

Note If you delete an IP pool that has users assigned to it, those users cannot authenticate until you edit the user profile and change their IP assignment settings. Alternately, if the users receive their IP assignment based on group membership, you can edit the user group profile and change the IP assignment settings for the group.

To delete an IP pool, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

Result: The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Click the name of the IP pool you need to delete.

Result: The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use column displays the number of IP addresses of this pool that are currently assigned to a user. The Available column displays the number of IP addresses currently not assigned to users.

Step 4 Click **Delete**.

Result: Cisco Secure ACS displays a dialog box to confirm that you want to delete the IP pool.

Step 5 To continue with deleting the IP pool, click **OK**.

Result: The IP pool is deleted. The AAA Server IP Pools table does not list the deleted IP pool.

IP Pools Address Recovery

The IP Pools Address Recovery feature enables you to recover assigned IP addresses that have not been used for a specified period of time. If Cisco Secure ACS is to reclaim the IP addresses correctly, an accounting network must be configured on the AAA client.

Enabling IP Pool Address Recovery

To enable IP pool address recovery, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Address Recovery**.

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **IP Pools** check box.

Result: The IP Address Recovery page appears.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select the **Release address if allocated for longer than** *X* **hours** check box and in the *X* box type the number of hours after which Cisco Secure ACS should recover assigned, unused IP addresses.

Step 4 Click **Submit**.

Result: Cisco Secure ACS implements the IP pools address recovery settings you made.

VoIP Accounting Configuration

The VoIP Accounting Configuration feature enables you to specify which accounting logs receive VoIP accounting data. There are three options for VoIP accounting:

- **Send to both RADIUS and VoIP Accounting Log Targets—**Cisco Secure ACS appends VoIP accounting data to the RADIUS accounting data and logs it separately to a CSV file. To view the data, you can use either RADIUS Accounting or VoIP Accounting under Reports and Activity.
- **Send only to VoIP Accounting Log Targets—**Cisco Secure ACS only logs VoIP accounting data to a CSV file. To view the data, you can use VoIP Accounting under Reports and Activity.
- **Send only to RADIUS Accounting Log Targets—**Cisco Secure ACS only appends VoIP accounting data to the RADIUS accounting data. To view the data, you can use RADIUS Accounting under Reports and Activity.

Downloaded from www.Manualslib.com manuals search engine

Configuring VoIP Accounting

Note The VoIP Accounting Configuration feature does not enable VoIP accounting. To enable VoIP accounting, see Chapter 9, "Working with Logging and Reports."

To configure VoIP accounting, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **VoIP Accounting Configuration**.

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Voice-over-IP (VoIP) Accounting Configuration** check box.

Result: The VoIP Accounting Configuration page appears. The Voice-over-IP (VoIP) Accounting Configuration table displays the options for VoIP accounting.

Step 3 Select the VoIP accounting option you want.

Step 4 Click **Submit**.

Result: Cisco Secure ACS implements the VoIP accounting configuration you specified.

Cisco Secure ACS Certificate Setup

Cisco Secure ACS provides an Extended Authentication Protocol Transport Level Security (EAP-TLS) feature for user authentication using digital certificates in RADIUS. With EAP-TLS, the same enterprise PKI (public key infrastructure) system and user certificates deployed for secure e-mail, Internet, or desktop security can be used for RADIUS user authentication.

Downloaded from www.Manualslib.com manuals search engine

Background on Certification

EAP and TLS are both IETF RFC standards. The EAP protocol extends the network point-to-point protocol (PPP) by providing new methods for carrying authentication information before establishing PPP connections, specifically, EAPOL (the encapsulation of EAP over LANs as established by IEEE 802.1X). In addition to digital certificates, EAP has methods for username and password authentication (that is, EAP-MD5 Challenge). TLS is the next generation SSL security protocol. TLS provides a way to use certificates for both user authentication, and for dynamic ephemeral session key generation. For more detailed information on EAP, TLS, and EAP-TLS, refer to the following IETF RFCs: PPP Extensible Authentication Protocol (EAP) RFC 2284, The TLS Protocol RFC 2246, and PPP EAP TLS Authentication Protocol RFC 2716.

Digital certificates are particularly useful because they do not require the sharing of secrets nor stored database credentials, can be scaled and trusted over large deployments, and can serve as a "two-factor" method of authentication that is stronger and more secure than shared secret systems. Mutual trust requires that Cisco Secure ACS have an installed certificate that can be verified by AAA clients and that a user attempting authentication via EAP-TLS bears a certificate from a trusted certification authority (CA). For authentication of a user to occur, the subject name contained in the user certificate must be identical to the username in the Cisco Secure ACS database (or the external LDAP Directory or Windows 2000 database that Cisco Secure ACS uses). Cisco Secure ACS requires that certificates and CA files used be in Base64-encoded X.509 version 3.

A user who is authenticated using EAP-TLS can then be mapped to user or group authorization information kept in the CiscoSecure user database, or in the Windows 2000 or generic LDAP Directory Server. Your Cisco Secure ACS must be installed on a Windows 2000 server (not Windows NT) if you intend to use EAP-TLS in conjunction with a Windows 2000 user database.

EAP-TLS requires support from both the end client and the AAA client. An example of an EAP-TLS client includes the Windows XP operating system; EAP-TLS compliant AAA clients include Cisco 802.1x-enabled switch platforms (such as the Catalyst 6000 product line), and Cisco Aironet Wireless solutions. In addition, Cisco Secure ACS needs to generate or enroll into an existing PKI and be granted an X.509 v3 digital certificate.

Downloaded from www.Manualslib.com manuals search engine

EAP-TLS Setup Overview

This section outlines the basic steps necessary to implement EAP-TLS in Cisco Secure ACS.

- Obtain, and install on Cisco Secure ACS, a "server" certificate. You can perform the "server" certificate installation using either the manual enrollment procedure or automatic enrollment procedure in this section.
- Install a certificate for the CA that issued the Cisco Secure ACS "server" certificate. For more information, see the "Certification Authority Setup" section on page 8-70.
- Ensure that any CA that you want to allow users to employ is listed in the Cisco Secure ACS's certificate trust list (CTL). For more information see the "Editing the Certificate Trust List" section on page 8-72.
- Verify that users you intend to authenticate using EAP-TLS reside in a database that supports EAP-TLS (CiscoSecure user database, Windows 2000 database, or generic LDAP database only).
- Verify that the user account names in Cisco Secure ACS match the subject field in each user certificate.
- Confirm that you have configured authentication options for EAP-TLS and then restart Cisco Secure ACS. For more detailed information see the "Global Authentication Setup" section on page 8-73.

Requirements for Certificate Enrollment

Cisco Secure ACS supports a variety of PKIs for digital certificate enrollment. To use the ACS general certificate enrollment feature, the following conditions apply:

- You must have a CA capable of handling PKCS #10 certificate requests if you intend to use Cisco Secure ACS to generate the certificate request.
- You must only employ certificates that meet the X.509 v3 digital certificate standard.
- The certificate's intended purpose must include server authentication.

Downloaded from www.Manualslib.com manuals search engine

This section contains procedures for the following subjects:

- Generating a Request for a Certificate, page 8-64
- Installing Cisco Secure ACS Certification with Manual Enrollment, page 8-66
- Installing Cisco Secure ACS Certification with Automatic Enrollment, page 8-68
- Performing Cisco Secure ACS Certification Update or Replacement, page 8-69

Generating a Request for a Certificate

You perform this generation procedure to create an RSA key pair for the server and a new digital certificate for Cisco Secure ACS, and to send information to a CA, requesting that they assign the server certificate for your Cisco Secure ACS. All EAP-TLS authentications require certificates from both the end-user clients and the Cisco Secure ACS(s) configured for EAP-TLS support. To obtain a server certificate, you can either import an existing server certificate into Cisco Secure ACS, or generate a new one. You do not need to perform this procedure from within Cisco Secure ACS if you have alternative means of generating a certificate request (including producing private and public key pairs). Note that one server certificate may be used for more than one Cisco Secure ACS by exporting the certificate and keypair from one server and importing this credential into additional Cisco Secure ACS(s).

Note If you are using a file to install a certificate in Cisco Secure ACS, the certificate must comply with the X.509 version 3 digital certificate standard.

To request a certificate for manual enrollment, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Result: If you are accessing this page for the first time, Cisco Secure ACS displays the Install new certificate table on the ACS Certificate Setup page. (If you have already installed a server certificate, information on it is displayed.)

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select the **Manual certificate enrollment** option.

Step 4 To have Cisco Secure ACS generate a certificate signing request (CSR), follow these steps:

a. Select the **Generate certificate signing request (CSR)** option.

b. In the **Certificate subject** box, type **cn=** followed by the name that you would like to use as subject name in this ACS certificate, for example, **cn=ACSWireless**.

c. In the **Private key file** box, type the full directory path and name of the file in which the private key is saved, for example, `c:\privateKeyFile.pem`.

Tip This private key is used later in the certificate installation process.

d. In the **Private key password** box, type the private key password (that you have invented).

e. In the **Retype private key password** box, retype the private key password.

f. From the **Key length** list, select the length of the key to be used.

Tip The choices for Key length are 512 or 1024 bits. The default and more secure choice is 1024 bits.

g. From the **Digest to sign with** list, select the digest (or hashing algorithm).

Tip The choices for **Digest to sign with** are MD2, MD5, SHA, and SHA1. The default is SHA1.

Step 5 Click **Submit**.

Result: Cisco Secure ACS prepares a certification signing request and displays it in the display area, on the right, under a banner that reads:

```
Now your certificate signing request is ready. You can copy and paste
it into any certification authority enrollment tool.
```


Downloaded from www.Manualslib.com manuals search engine

Step 6 Open a browser window and navigate to the web site of your CA. Then copy the encoded certificate signing request from Cisco Secure ACS and paste it into the CA submission form, as applicable.

Result: The CA receives the request and issues a certificate.

Tip Typically, the CA generates the certificate and provides the means for you to download it.

Installing Cisco Secure ACS Certification with Manual Enrollment

You perform this procedure to install a Cisco Secure ACS certificate.

Before You Begin

You must have a server certificate for your Cisco Secure ACS before you can install it. You can use the procedure in the "Generating a Request for a Certificate" section on page 8-64, or any other means to obtain a certificate for manual installation.

If you are using Microsoft Windows 2000 Certificate Services to obtain your server certificate, you can do it using the procedure in the "Installing Cisco Secure ACS Certification with Automatic Enrollment" section on page 8-68, or you can generate the request using the MS Certificate Services web interface. For more information refer to the "EAP-TLS Deployment Guide," which can be found on the Cisco Secure ACS Product Literature site:

http://www.cisco.com/warp/public/cc/pd/sqsw/sq/prodlit/index.shtml

To install an existing certificate for use on Cisco Secure ACS, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Result: Cisco Secure ACS displays the Install new certificate table on the ACS Certificate Setup page.

Step 3 Select the **Manual certificate enrollment** option.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Select the **Use existing certificate** option.

Step 5 You must specify whether the system should read the certificate from a specified file or use a certificate already in storage on the local machine. Do one of the following:

a. To specify that Cisco Secure ACS should read the certificate from a specified file, select the **Read certificate from file** option, and then type the full directory path and name of the certificate file in the Certificate file box.

b. To specify that Cisco Secure ACS should use a particular existing certificate from local machine storage, select the **Use certificate from storage** option, and then type the certificate CN (common name/subject name) in the Certificate CN box (without the *"cn="* prefix).

Step 6 If you generated the request using Cisco Secure ACS, in the Private key file box, type the full directory path and name of the file that contains the private key.

Note If the certificate was installed in storage with the private key, you do not have the private key file and do not need to type it.

Tip This is the private key associated with the server certificate.

Step 7 In the Private key password box, type the private key password.

Step 8 Click **Submit**.

Result: To show that the certificate setup is complete, Cisco Secure ACS displays the Installed Certificate Information table, which contains the following certificate information:

- Issued to: *certificate subject*
- Issued by: *CA common name*
- Valid from:
- Valid to:
- Validity

Downloaded from www.Manualslib.com manuals search engine

Installing Cisco Secure ACS Certification with Automatic Enrollment

You can use this process to install ACS certification using your existing Microsoft enterprise CA.

Before You Begin

To employ the Cisco Secure ACS automatic certificate enrollment feature, the following conditions apply:

- You must be using Microsoft Windows 2000 Certificate Services
- Your Cisco Secure ACS must be installed on a Windows 2000 server (not Windows NT)
- Your Cisco Secure ACS must be part of the same domain as the Microsoft enterprise CA, or it must belong to a domain that has a trust relationship with the domain that the Microsoft Enterprise CA belongs to
- You must provide Cisco Secure ACS with an administrator login and password for the domain to which Cisco Secure ACS belongs

To use automatic enrollment to install a new ACS certificate, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Result: Cisco Secure ACS displays the Install new certificate table on the ACS Certificate Setup page.

Note If your Cisco Secure ACS has already been enrolled with a certificate, you will not see the Install new certificate table. Rather, you would see the Installed Certificate Information table.

Step 3 Select the **Automatic certificate enrollment** option in the lower portion of the page.

Downloaded from www.Manualslib.com manuals search engine

Step 4 To specify the Microsoft CA, under Microsoft Windows 2000 Certificate Services, follow these steps:

a. In the CA server name box, type the name of the CA server.

b. In the CA common name box, type the common name of the CA.

c. In the **Certificate subject** box, type the name you want to use as subject name for the Cisco Secure ACS certificate.

Step 5 In the Administrative login box, type the login name.

Step 6 In the Password box, type the password.

Step 7 Click **Submit**.

Result: To show that the certificate setup is complete, Cisco Secure ACS displays the Installed Certificate Information table, which contains the following certificate information:

- Issued to: *certificate subject*
- Issued by: *CA common name*
- Valid from:
- Valid to:
- Validity

Performing Cisco Secure ACS Certification Update or Replacement

You can use this process to update or replace an existing Cisco Secure ACS certificate that is out-of-date or out-of-order.

Warning **This procedure eliminates your existing Cisco Secure ACS certificate.**

To install a new ACS certificate, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Downloaded from www.Manualslib.com manuals search engine

Result: Cisco Secure ACS displays the Installed Certificate Information table on the ACS Certificate Setup page.

Note If your Cisco Secure ACS has not already been enrolled with a certificate, you do not see the Installed Certificate Information table. Rather, you see the Install new certificate table. If this is the case, you can proceed to Step 5.

Step 3 Click Enroll New Certificate.

Result: A confirmation dialog box appears.

Step 4 To confirm that you intend to enroll a new certificate, click **OK**.

Result: The existing Cisco Secure ACS certificate is removed.

Step 5 You can now install the replacement certificate in the same manner as an original certificate. For detailed procedural information, see the "Installing Cisco Secure ACS Certification with Manual Enrollment" section on page 8-66 or the "Installing Cisco Secure ACS Certification with Automatic Enrollment" section on page 8-68.

Certification Authority Setup

Cisco Secure ACS comes preconfigured with a list of popular CAs, none of which are enabled until you explicitly signify trustworthiness. To specify one or more CAs as trusted for user certification, you perform the procedure in the "Editing the Certificate Trust List" section on page 8-72.

You perform the procedure in the "Adding a New CA Certificate to Local Certificate Storage" section on page 8-72 to add a new CA to your certificate trust list (CTL).

Cisco Secure ACS uses the CTL to verify the client certificates. Only certificates that were issued by a CA that exists in the Cisco Secure ACS CTL are trusted by Cisco Secure ACS. If all the clients and Cisco Secure ACS are getting their certificates from the same CA you do not need to add any CA to the CTL because Cisco Secure ACS automatically trusts the CA that issues its certificate. You do need to install the certificate for the CA that issued the Cisco Secure ACS Server Certificate, but there is no need to add it to the CTL.

Downloaded from www.Manualslib.com manuals search engine

This section contains procedures for the following subjects:

- Editing the Certificate Trust List, page 8-72
- Adding a New CA Certificate to Local Certificate Storage, page 8-72

Note The CAs on the CTL should be those that issue user certificates that you want Cisco Secure ACS to recognize as trustworthy.

Trust Requirements and Models

TLS authentications require two elements of trust. The first element of trust is when the TLS negotiation establishes end-user trust by validating, through RSA signature verifications, that the user is in possession of a keypair signed by a certificate. This verifies that the end user is the legitimate keyholder for a given digital certificate and corresponding user identification contained in the certificate. However, trusting that a user is in possession of a certificate only provides a username/keypair binding. The second element of trust is to use a third-party signature (usually from a CA) that verifies the information in a certificate. This third-party binding is similar to the real world equivalent of the U.S. Passport seal on your passport. You trust the passport because you trust the preparation and identity checking that the passport office made when creating that passport. You trust digital certificates by installing the root certificate CA signature in an equivalent way.

How you edit your CTL determines the type of trust model you have. Many employ a restricted trust model wherein very few, privately controlled CAs are trusted. This model provides the highest level of security but restricts adaptability and expandability. The alternative, an open trust model, allows for more CAs or public CAs. This open trust model trades off increased security for greater adaptability and expandability.

We recommend that you fully understand the implications of your trust model before editing the CTL in Cisco Secure ACS.

Downloaded from www.Manualslib.com manuals search engine

Editing the Certificate Trust List

You use this procedure to add CAs to or remove CAs from your CTL.

To edit the CTL, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Certification Authority Setup**.

Result: Cisco Secure ACS displays the CA Operations table.

Step 3 To edit the certificate trust list, click **Edit certificate trust list**.

Result: The system displays the Edit the Certificate Trust List (CTL) table.

Warning **Adding a public CA that you do not control may reduce your system security. For more information, see the "Trust Requirements and Models" section on page 8-71.**

Step 4 To add a CA to your CTL, select corresponding check box.

Tip You can select, or deselect, as many CAs as you want.

Step 5 Click **Submit**.

Result: Cisco Secure ACS adds (or removes) the specified CA to (or from) the CTL.

Adding a New CA Certificate to Local Certificate Storage

Use this procedure to add a new certificate to local certificate storage.

You must perform this procedure for the CA that issued your server certificate to distinguish it from CAs trusted to issue user certification.

Downloaded from www.Manualslib.com manuals search engine

Note Cisco Secure ACS requires that the certificate and CA files be in Base64-encoded X.509. You can also add the CA certificate by installing it outside of Cisco Secure ACS (in Windows). After you install it, you should be able to see the new CA in the CA list from within Cisco Secure ACS.

To add a new CA certificate to local certificate storage, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Certification Authority Setup**.

Result: Cisco Secure ACS displays the CA Operations table.

Step 3 In the CA file name box, type the full directory path and name of the CA certificate file.

Step 4 Click **Submit**.

Result: Cisco Secure ACS displays the following message in the display area on the right:

```
New CA certificate is successfully added into the global system
certificate storage.
```

After you have installed a certificate in Cisco Secure ACS and added the required CAs, you can configure EAP-TLS in Global Authentication Setup and then restart Cisco Secure ACS.

Global Authentication Setup

Use this procedure to select and configure how Cisco Secure ACS handles extended options for authentication. In particular, you use this procedure to allow either EAP-MD5 or EAP-TLS, and to allow either MS-CHAP Version 1 or MS-CHAP Version 2, or both.

Downloaded from www.Manualslib.com manuals search engine

To configure authentication options, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Global Authentication Setup**.

Result: Cisco Secure ACS displays the Global Authentication Setup page.

Step 3 In the EAP Configuration table, select one of the following options:

- Allow EAP-MD5-Challenge
- Allow EAP-TLS (requires server certificate)

Step 4 In the **MS-CHAP Configuration** table, select each version of MS-CHAP that you want to allow for Cisco Secure ACS. Your choices are the following:

- Allow MS-CHAP Version 1 Authentication
- Allow MS-CHAP Version 2 Authentication

Step 5 Click **Submit + Restart**.

Result: Cisco Secure ACS restarts its services and implements the authentication configuration options you selected.

Downloaded from www.Manualslib.com manuals search engine

Working with Logging and Reports

Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) produces a wide variety of logs and provides a way to view most of these logs in the Cisco Secure ACS HTML interface as HTML reports. This chapter contains the following topics about logging:

- Logging Formats, page 9-1
- Special Logging Attributes, page 9-2
- Update Packets In Accounting Logs, page 9-3
- About Cisco Secure ACS Logs and Reports, page 9-4
- Working with CSV Logs, page 9-19
- Working with ODBC Logs, page 9-25
- Remote Logging, page 9-29
- Service Logs, page 9-34

Logging Formats

Cisco Secure ACS logs a variety of user and system activities. Depending on the log, and how you have configured Cisco Secure ACS, logs can be recorded in one of two formats:

- **Comma-separated value (CSV) files—**The CSV format records data in columns separated by commas. This format is easily imported into a variety of third-party applications, such as Microsoft Excel or Microsoft Access. After data from a CSV file is imported into such applications, you can prepare

Downloaded from www.Manualslib.com manuals search engine

charts or perform queries, such as determining how many hours a user was logged in to the network during a given period. For information about how to use a CSV file in a third-party application such as Microsoft Excel, please see the documentation supplied by the third-party vendor. You can access the CSV files either on the Cisco Secure ACS server hard drive or by downloading the CSV file from the HTML interface. For more information about downloading the CSV file from the HTML interface, see the "Viewing a CSV Report" section on page 9-20.

- **ODBC-compliant database tables—**ODBC logging enables you to configure Cisco Secure ACS to log directly in an ODBC-compliant relational database, where it is stored in tables, one table per log. After the data is exported to the relational database, you can use the data however you need. For more information about querying the data in your relational database, refer to the documentation supplied by the relational database vendor.

For information about the formats available for a specific log, see the "About Cisco Secure ACS Logs and Reports" section on page 9-4.

Special Logging Attributes

Among the many attributes that Cisco Secure ACS can record in its CSV or ODBC logs, a few are of special importance. The following list explains the special logging attributes provided by Cisco Secure ACS.

- **User-defined attributes**—These logging attributes appear in the Attributes list for any log configuration page. Cisco Secure ACS lists them using their default names: Real Name, Description, User Field 3, User Field 4, and User Field 5. If you change the name of a user-defined attribute, the default name still appears in the Attributes list rather than the new name.

  The content of these attributes is determined by the values entered in the corresponding fields in the user account. For more information about user-defined attributes, see the "User Data Configuration Options" section on page 3-3.

- **ExtDB Info—**If the user is authenticated with an external user database, this attribute contains a value returned by the database. In the case of a Windows NT/2000 user database, this attribute contains the name of the domain that authenticated the user.

Downloaded from www.Manualslib.com manuals search engine

For more information about configuring the content of CSV logs, see the "Configuring a CSV Log" section on page 9-22. For more information about configuring the content of an ODBC log, see the "Configuring an ODBC Log" section on page 9-27.

- **Access Device**—The name of the AAA client sending the logging data to Cisco Secure ACS.
- **Network Device Group**—The network device group to which the access device (AAA client) belongs.
- **Filter Information**—The result of network access restrictions (NARs) applied to the user, if any. The message in this field indicates whether all applicable NARs permitted the user access, all applicable NARs denied the user access, or more specific information about which NAR denied the user access. If no NARs apply to the user, this logging attribute notes that no NARs were applied.

  The Filter Information attribute is available for Passed Authentication and Failed Attempts logs.
- **Device Command Set**—The name of the device command set, if any, that was used to satisfy a command authorization request.

  The Device Command Set attribute is available for Passed Authentication and Failed Attempts logs.

Update Packets In Accounting Logs

Whenever you configure Cisco Secure ACS to record accounting data for user sessions, Cisco Secure ACS records start and stop packets. If you want, you can configure Cisco Secure ACS to record update packets, too. In addition to providing interim accounting information during a user session, update packets drive password expiry messages via CiscoSecure Authentication Agent. In this use, the update packets are referred to as watchdog packets.

Note To record update packets in Cisco Secure ACS accounting logs, you must configure your AAA clients to send the update packets. For more information about configuring your AAA client to send update packets, refer to the documentation for your AAA clients.

Downloaded from www.Manualslib.com manuals search engine

- **Logging Update Packets Locally—**To log update packets on the local Cisco Secure ACS server, enable the Log Update/Watchdog Packets from this Access Server option for each AAA client in Network Configuration.

  For more information on setting this option for a AAA client, see the "Adding and Configuring a AAA Client" section on page 4-9.

- **Logging Update Packets Remotely—**To log update packets on a remote logging server, enable the Log Update/Watchdog Packets from this remote AAA Server option for the remote server's AAA Server table entry on the local Cisco Secure ACS server.

  For more information on setting this option for a AAA server, see the "Adding and Configuring a AAA Server" section on page 4-16.

About Cisco Secure ACS Logs and Reports

The logs that Cisco Secure ACS provides can be divided into four groups:

- Accounting Logs, page 9-4
- Dynamic Cisco Secure ACS Administration Reports, page 9-10
- Cisco Secure ACS System Logs, page 9-15
- Service Logs, page 9-34

This section contains information about the first three groups. For information about service logs, see the "Service Logs" section on page 9-34.

Accounting Logs

Accounting logs contain information about the use of remote access services by users. By default, these logs are available in CSV format. With the exception of the Passed Authentications log, you can also configure Cisco Secure ACS to export the data for these logs to an ODBC-compliant relational database that you configure to store the log data.

The accounting logs include:

- TACACS+ Accounting Log, page 9-5
- TACACS+ Administration Log, page 9-6

Downloaded from www.Manualslib.com manuals search engine

- RADIUS Accounting Log, page 9-7
- VoIP Accounting Log, page 9-8
- Failed Attempts Log, page 9-9
- Passed Authentications Log, page 9-10

TACACS+ Accounting Log

The TACACS+ Accounting log contains the following information:

- User sessions stop and start times
- AAA client messages with username
- Caller line identification information
- Session duration

Topics regarding this log include the following:

- **Enabling a TACACS+ Accounting Log**—You can enable the TACACS+ Accounting log in either CSV or ODBC format.
  - **CSV—**For instructions on how to enable the TACACS+ Accounting log in CSV format, see the "Enabling or Disabling a CSV Log" section on page 9-19.
  - **ODBC—**For instructions on how to enable the ODBC TACACS+ Accounting log, see the "Configuring an ODBC Log" section on page 9-27.
- **Viewing a TACACS+ Accounting Report—**For instructions on viewing the TACACS+ Accounting report in the HTML interface, see the "Viewing a CSV Report" section on page 9-20.

Downloaded from www.Manualslib.com manuals search engine

- **Configuring a TACACS+ Accounting Log—**The steps for configuring a TACACS+ Accounting log vary depending upon which format you want to use. For more information about log formats, see the "Logging Formats" section on page 9-1.
  - **CSV—**The default location for CSV TACACS+ Accounting files is `Program Files\CiscoSecure ACS v`*x.x*`\Logs\TACACS+Accounting`.

    For instructions on configuring the CSV TACACS+ Accounting log, see the "Configuring a CSV Log" section on page 9-22.
  - **ODBC—**For instructions on configuring the ODBC TACACS+ Accounting log, see the "Configuring an ODBC Log" section on page 9-27.

TACACS+ Administration Log

The TACACS+ Administration log lists configuration commands entered on a AAA client using TACACS+ (Cisco IOS). Particularly if you use Cisco Secure ACS to perform command authorization, we recommend that you use this log.

Note To use the TACACS+ Administration log, your TACACS+ AAA clients must be configured to perform command accounting with Cisco Secure ACS.

Topics regarding this log include the following:

- **Enabling a TACACS+ Administration Log—**You can enable the TACACS+ Administration log in either CSV or ODBC format.
  - **CSV—**For instructions on how to enable the TACACS+ Administration log in CSV format, see the "Enabling or Disabling a CSV Log" section on page 9-19.
  - **ODBC—**For instructions on how to enable the ODBC TACACS+ Administration log, see the "Configuring an ODBC Log" section on page 9-27.
- **Viewing a TACACS+ Administration Report—**For instructions on viewing the TACACS+ Administration report in the HTML interface, see the "Viewing a CSV Report" section on page 9-20.

Downloaded from www.Manualslib.com manuals search engine

- **Configuring a TACACS+ Administration Log—**The steps for configuring a TACACS+ Administration log vary depending upon which format you want to use. For more information about log formats, see the "Logging Formats" section on page 9-1.
  - **CSV—**The default location for CSV TACACS+ Administration files is `Program Files\CiscoSecure ACS v`*x.x*`\Logs\TACACS+Administration`.

    For instructions on configuring the CSV TACACS+ Administration log, see the "Configuring a CSV Log" section on page 9-22.
  - **ODBC—**For instructions on configuring the ODBC TACACS+ Administration log, see the "Configuring an ODBC Log" section on page 9-27.

RADIUS Accounting Log

The RADIUS Accounting log contains the following information:

- User sessions stop and start times
- AAA client messages with username
- Caller line identification information
- Session duration

You can configure Cisco Secure ACS to include accounting for Voice over IP (VoIP) in the RADIUS Accounting log, in a separate VoIP accounting log, or in both places.

Topics regarding this log include the following:

- **Enabling a RADIUS Accounting Log**—You can enable the RADIUS Administration log in either CSV or ODBC format.
  - **CSV—**For instructions on how to enable the RADIUS Accounting log in CSV format, see the "Enabling or Disabling a CSV Log" section on page 9-19.
  - **ODBC—**For instructions on how to enable the ODBC RADIUS Accounting log, see the "Configuring an ODBC Log" section on page 9-27.
- **Viewing a RADIUS Accounting Report—**For instructions on viewing the RADIUS Accounting report in the HTML interface, see the "Viewing a CSV Report" section on page 9-20.

Downloaded from www.Manualslib.com manuals search engine

- **Configuring a RADIUS Accounting Log—**The steps for configuring a RADIUS Accounting log vary depending upon which format you want to use. For more information about log formats, see the "Logging Formats" section on page 9-1.
  - **CSV—**The default location for CSV RADIUS Accounting files is `Program Files\CiscoSecure ACS v`*x.x*`\Logs\RADIUSAccounting`.

    For instructions on configuring the CSV RADIUS Accounting log, see the "Configuring a CSV Log" section on page 9-22.
  - **ODBC—**For instructions on configuring the ODBC RADIUS Accounting log, see the "Configuring an ODBC Log" section on page 9-27.

VoIP Accounting Log

The VoIP Account log contains the following information:

- VoIP session stop and start times
- AAA client messages with username
- Caller line identification (CLID) information
- VoIP session duration

You can configure Cisco Secure ACS to include accounting for VoIP in this separate VoIP accounting log, in the RADIUS Accounting log, or in both places.

Topics regarding this log include the following:

- **Enabling a VoIP Accounting Log**—You can enable the VoIP Accounting log in either CSV or ODBC format.
  - **CSV—**For instructions on how to enable the VoIP Accounting log in CSV format, see the "Enabling or Disabling a CSV Log" section on page 9-19.
  - **ODBC—**For instructions on how to enable the ODBC VoIP Accounting log, see the "Configuring an ODBC Log" section on page 9-27.
- **Viewing a VoIP Accounting Report—**For instructions on viewing the VoIP Accounting report in the HTML interface, see the "Viewing a CSV Report" section on page 9-20.

Downloaded from www.Manualslib.com manuals search engine

- **Configuring a VoIP Accounting Log—**The steps for configuring a VoIP Accounting log vary depending upon which format you want to use. For more information about log formats, see the "Logging Formats" section on page 9-1.
  - **CSV—**The default location for CSV VoIP Accounting files is `Program Files\CiscoSecure ACS v`*x.x*`\Logs\VoIP Accounting`.

    For instructions on configuring the CSV VoIP Accounting log, see the "Configuring a CSV Log" section on page 9-22.
  - **ODBC—**For instructions on configuring the ODBC VoIP Accounting log, see the "Configuring an ODBC Log" section on page 9-27.

Failed Attempts Log

The Failed Attempts log lists authentication and authorization failures with an indication of the cause.

Topics regarding this log include the following:

- **Enabling a Failed Attempts Log—**You can enable the Failed Attempts log in either CSV or ODBC format.
  - **CSV—**For instructions on how to enable the Failed Attempts log in CSV format, see the "Enabling or Disabling a CSV Log" section on page 9-19.
  - **ODBC—**For instructions on how to enable the ODBC Failed Attempts log, see the "Configuring an ODBC Log" section on page 9-27.
- **Viewing a Failed Attempts Report—**For instructions on viewing the Failed Attempts report in the HTML interface, see the "Viewing a CSV Report" section on page 9-20.
- **Configuring a Failed Attempts Log**—The steps for configuring a Failed Attempts log vary depending upon which format you want to use. For more information about log formats, see the "Logging Formats" section on page 9-1.
  - **CSV—**The default location for CSV Failed Attempts files is `Program Files\CiscoSecure ACS v`*x.x*`\Logs\Failed Attempts`.

    For instructions on configuring the CSV Failed Attempts log, see the "Configuring a CSV Log" section on page 9-22.
  - **ODBC—**For instructions on configuring the ODBC Failed Attempts log, see the "Configuring an ODBC Log" section on page 9-27.

Downloaded from www.Manualslib.com manuals search engine

Passed Authentications Log

The Passed Authentications log lists successful authentication requests. This log is not dependent upon accounting packets from your AAA clients, so it is available even if your AAA clients do not support RADIUS accounting or if you have disabled accounting on your AAA clients.

Topics regarding this log include the following:

- **Enabling a Passed Authentications Log—**For instructions on how to enable the Passed Authentications log, see the "Enabling or Disabling a CSV Log" section on page 9-19.
- **Viewing a Passed Authentications Report—**For instructions on viewing the Passed Authentications report in the HTML interface, see the "Viewing a CSV Report" section on page 9-20.
- **Configuring a Passed Authentications Log**—The Passed Authentications log is available as a CSV file, viewable in the HTML interface.

  The default location for Passed Authentications files is `Program Files\CiscoSecure ACS` *x.x*`\Logs\Passed Authentications`.

  For instructions on configuring the CSV Passed Authentications log, see the "Configuring a CSV Log" section on page 9-22.

Dynamic Cisco Secure ACS Administration Reports

These reports show the status of user accounts at the moment they are accessed. They are available only in the Cisco Secure ACS HTML interface.

The Dynamic Cisco Secure ACS Administration reports include:

- Logged-In Users Report, page 9-11
- Disabled Accounts Report, page 9-14

Downloaded from www.Manualslib.com manuals search engine

Logged-In Users Report

The Logged-in Users report lists all users currently receiving services for a single AAA client or all AAA clients with access to Cisco Secure ACS.

Note To use the logged-in user list feature, your AAA client must perform authentication and accounting using the same protocol—either TACACS+ or RADIUS.

Topics regarding this report include the following:

- **Enabling a Logged-in Users Report—**The Logged-in Users report is always enabled. You cannot disable this report.
- **Viewing a Logged-in Users Report—**For instructions on viewing the Logged-in User report in the HTML interface, see the "Viewing the Logged-in Users Report" section on page 9-11.
- **Configuring a Logged-in Users Report—**The Logged-in Users report is only available in the HTML interface. There are no configuration options for the Logged-in Users report.
- **Deleting Logged-in Users**—For instructions about deleting logged-in users from specific AAA clients or from all AAA clients, see the "Deleting Logged-in Users" section on page 9-12.

Viewing the Logged-in Users Report

To view the Logged-in Users report, follow these steps:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Logged-in Users**.

Result: The Select a AAA Client page displays the name of each AAA client, its IP address, and the number of users logged in through the AAA client. At the bottom of the table, the All AAA Clients entry shows the total number of users logged in.

Downloaded from www.Manualslib.com manuals search engine

Tip You can sort the table by any column's entries, in either ascending or descending order. Click a column title once to sort the table by that column's entries in ascending order. Click the column a second time to sort the table by that column's entries in descending order.

Step 3 Do one of the following:

a. To see a list of all users logged in, click **All AAA Clients**.

b. To see a list of users logged in through a particular AAA client, click the name of the AAA client.

Result: Cisco Secure ACS displays a table of users logged in, including the following information:

- Date and Time
- User
- Group
- Assigned IP
- Port
- Source AAA Client

Tip You can sort the table by any column's entries, in either ascending or descending order. Click a column title once to sort the table by that column's entries in ascending order. Click the column a second time to sort the table by that column's entries in descending order.

Deleting Logged-in Users

From a Logged-in Users Report, you can instruct Cisco Secure ACS to delete users logged into a specific AAA client. When a user session terminates without a AAA client sending an accounting stop packet to the Cisco Secure ACS server, the Logged-in Users Report continues to show the user. Deleting logged-in users from a AAA client ends the accounting for those user sessions.

Downloaded from www.Manualslib.com manuals search engine

Note Deleting logged-in users only ends the Cisco Secure ACS accounting record of users logged in to a particular AAA client. It does not terminate active user sessions, nor does it affect user records.

To delete logged-in users, follow these steps:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Logged-in Users**.

Result: The Select a AAA Client page displays the name of each AAA client, its IP address, and the number of users logged in through the AAA client. At the bottom of the table, the All AAA Clients entry shows the total number of users logged in.

Step 3 Click the name of the AAA client whose users you want to delete from the Logged-in Users report.

Result: Cisco Secure ACS displays a table of all users logged in through the AAA client. The Purge Logged in Users button appears below the table.

Step 4 Click **Purge Logged in Users**.

Result: Cisco Secure ACS displays a message, indicating the number of users purged from the report and the IP address of the AAA client.

Downloaded from www.Manualslib.com manuals search engine

Disabled Accounts Report

The Disabled Accounts report lists all user accounts that are currently disabled and the reason they were disabled.

Topics regarding this report include the following:

- **Enabling a Disabled Accounts Report—**The Disabled Accounts report is always enabled. You cannot disable this report.
- **Viewing a Disabled Accounts Report—**For instructions on viewing the Disabled Accounts report in the HTML interface, see the "Viewing the Disabled Accounts Report" section on page 9-14.
- **Configuring a Disabled Accounts Report—**The Disabled Accounts report is only available in the HTML interface. There are no configuration options for the Disabled Accounts report.

Viewing the Disabled Accounts Report

To view the Disabled Accounts report, follow these steps:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Disabled Accounts**.

Result: The Select a user account to edit page displays disabled user accounts, the account status, and the group to which the user account is assigned.

Step 3 To edit a user account listed, in the User column, click the username.

Result: Cisco Secure ACS opens the user account for editing.

For more information about editing a user account, see the "Basic User Setup Options" section on page 7-4.

Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS System Logs

The system logs are logs about the Cisco Secure ACS system and therefore record system-related events. These logs are primarily useful for troubleshooting or audits. They are only available in CSV format. The system logs include the following:

- ACS Backup and Restore Log, page 9-15
- RDBMS Synchronization Log, page 9-16
- Database Replication Log, page 9-16
- Administration Audit Log, page 9-17
- ACS Service Monitoring Log, page 9-18

ACS Backup and Restore Log

The ACS Backup and Restore log lists Cisco Secure ACS backup and restore activity.

Topics regarding this log include the following:

- **Enabling the ACS Backup and Restore Log—**The ACS Backup and Restore log is always enabled. You cannot disable this log.
- **Viewing an ACS Backup and Restore Report—**For instructions on viewing the Failed Attempts report in the HTML interface, see the "Viewing a CSV Report" section on page 9-20.
- **Configuring the ACS Backup and Restore Log—**The ACS Backup and Restore log is available as a CSV file, viewable in the HTML interface. There are no configuration options for the ACS Backup and Restore log.

  The default location for ACS Backup and Restore files is `Program Files\CiscoSecure ACS v`*`x.x`*`\Logs\Backup and Restore`.

Downloaded from www.Manualslib.com manuals search engine

RDBMS Synchronization Log

The RDBMS Synchronization log lists RDBMS Synchronization activity.

Topics regarding this log include the following:

- **Enabling the RDBMS Synchronization Log—**The RDBMS Synchronization log is always enabled. You cannot disable this log.
- **Viewing an RDBMS Synchronization Report**—For instructions on viewing the RDBMS Synchronization report in the HTML interface, see the "Viewing a CSV Report" section on page 9-20.
- **Configuring the RDBMS Synchronization Log—**The RDBMS Synchronization log is available as a CSV file, viewable in the HTML interface. There are no configuration options for the RDBMS Synchronization log.

  The default location for RDBMS Synchronization files is `Program Files\CiscoSecure ACS v`*x.x*`\Logs\DbSync`.

Database Replication Log

The Database Replication log lists database replication activity.

Topics regarding this log include the following:

- **Enabling the Database Replication Log—**The Database Replication log is always enabled. You cannot disable this log.
- **Viewing a Database Replication Report**—For instructions on viewing the Database Replication report in the HTML interface, see the "Viewing a CSV Report" section on page 9-20.
- **Configuring the Database Replication Log—**The Database Replication log is available as a CSV file, viewable in the HTML interface. There are no configuration options for the Database Replication log.

  The default location for RDBMS Synchronization files is `Program Files\CiscoSecure ACS v`*x.x*`\Logs\DBReplicate`.

Downloaded from www.Manualslib.com manuals search engine

Administration Audit Log

The Administration Audit log lists actions taken by each system administrator, such as adding users, editing groups, configuring a AAA client, or viewing reports.

Topics regarding this log include the following:

- **Enabling the Administration Audit Log—**The Administration Audit log is always enabled. You cannot disable this log.
- **Viewing an Administration Audit Report—**For instructions on viewing the Administration Audit report in the HTML interface, see the "Viewing a CSV Report" section on page 9-20.
- **Configuring the Administration Audit Log—**The Administration Audit log is available as a CSV file, viewable in the HTML interface.

  The default location for Administration Audit files is `Program Files\CiscoSecure ACS v`*x.x*`\Logs\AdminAudit`.

  For instructions on configuring the Administration Audit log, see the "Configuring the Administration Audit Log" section on page 9-17.

Configuring the Administration Audit Log

To configure the Administrative Audit log, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Step 2 Click **Audit Policy**.

Result: The Audit Policy Setup page appears.

Step 3 To generate a new Administrative Audit CSV file at a regular interval, select one of the following options:

- **Every day**—Cisco Secure ACS generates a new Administrative Audit CSV file at the start of each day.
- **Every week**—Cisco Secure ACS generates a new Administrative Audit CSV file at the start of each week.
- **Every month**—Cisco Secure ACS generates a new Administrative Audit CSV file at the start of each month.

Downloaded from www.Manualslib.com manuals search engine

Step 4 To generate a new Administrative Audit CSV file when the current file reaches a specific size, select the **When size is greater than** *x* **KB** option and type the file size threshold in kilobytes in the *x* box.

Step 5 To manage which Administrative Audit CSV files Cisco Secure ACS keeps, follow these steps:

a. Select the **Manage Directory** check box.

b. To limit the number of Administrative Audit CSV files Cisco Secure ACS retains, select the **Keep only the last** *x* **files** option and type the number of files you want Cisco Secure ACS to retain in the *x* box.

c. To limit how old Administrative Audit CSV files retained by Cisco Secure ACS can be, select the **Delete files older than** *x* **days** option and type the number of days for which Cisco Secure ACS should retain a Administrative Audit CSV file before deleting it.

Step 6 Click **Submit**.

Result: Cisco Secure ACS saves and implements the Administrative Audit log settings you specified.

ACS Service Monitoring Log

The ACS Service Monitoring log lists when ACS services start and stop.

Topics regarding this log include the following:

- **Enabling the ACS Service Monitoring Log—**The Administration Audit log is always enabled. You cannot disable this log.
- **Viewing an ACS Service Monitoring Report—**For instructions on viewing the Administration Audit report in the HTML interface, see the "Viewing a CSV Report" section on page 9-20.
- **Configuring the ACS Service Monitoring Log—**For information about configuring the ACS Service Monitoring log, see the "Cisco Secure ACS Active Service Management" section on page 8-48.

  The default location for ACS Service Monitoring files is `Program Files\CiscoSecure ACS v`*`x.x`*`\Logs\ServiceMonitoring`.

Downloaded from www.Manualslib.com manuals search engine

Working with CSV Logs

This section contains the following topics:

- CSV Log File Names, page 9-19
- Enabling or Disabling a CSV Log, page 9-19
- Viewing a CSV Report, page 9-20
- Configuring a CSV Log, page 9-22

CSV Log File Names

When you access a report in Reports and Activity, Cisco Secure ACS lists the CSV files in chronological order, with the current CSV file at the top of the list. The current file is named *log*.csv, where *log* is the name of the log.

Older files are named in the following format:

log`yyyy-mm-dd.csv`

where

log is the name of the log.

yyyy is the year the CSV file was started.

mm is the month the CSV file was started, in numeric characters.

dd is the date the CSV file was started.

For example, a Database Replication log file that was generated on October 13, 1999, would be named `Database Replication 1999-10-13.csv`.

If you have selected the day-month-year format under Interface Configuration: Date Format Control, this log file would be named `Database Replication 1999-13-10.csv`.

Enabling or Disabling a CSV Log

This procedure describes how to enable or disable a CSV log. For instructions about configuring the content of a CSV log, see the "Configuring a CSV Log" section on page 9-22.

Downloaded from www.Manualslib.com manuals search engine

The logs to which this procedure applies are:

- TACACS+ Accounting Log
- TACACS+ Administration Log
- RADIUS Accounting Log
- VoIP Account Log
- Failed Attempts Log
- Passed Authentications log

To enable or disable a CSV log, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Logging**.

Step 3 Click the name of the CSV log you want to enable.

Result: The CSV *log* Comma-Separated Values File Configuration page appears, where *log* is the name of the CSV log you selected.

Step 4 To enable the log, under Enable Logging, select the **Log to CSV** *log* **report** check box, where *log* is the name of the CSV log you selected in Step 3.

Step 5 To disable the log, under Enable Logging, clear the **Log to CSV** *report* **log** check box, where *log* is the name of the CSV log you selected in Step 3.

Step 6 Click **Submit**.

Result: If you enabled the log, Cisco Secure ACS begins logging information for the log selected. If you disabled the log, Cisco Secure ACS stops logging information for the log selected.

Viewing a CSV Report

The reports to which this procedure applies are:

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting

Downloaded from www.Manualslib.com manuals search engine

- VoIP Accounting
- Failed Attempts
- Passed Authentications
- ACS Backup and Restore
- RDBMS Synchronization
- Database Replication
- Administration Audit
- ACS Service Monitoring

When you select Logged-in Users or Disabled Accounts, a list of logged-in users or disabled accounts appears in the display area, which is the frame on the right side of the web browser. For all other types of reports, a list of applicable reports appears. Files are listed in chronological order, with the most recent file at the top of the list. The reports are named and listed by the date on which they were created; for example, `1999-10-05.csv` was created on October 5, 1999.

Note If you select Day/Month/Year format, a file created on 5 October 1999 is named `1999-05-10`. For instructions, see the "Date Format Control" section on page 8-3.

Files in CSV format can be imported into spreadsheets using most popular spreadsheet application software. Refer to your spreadsheet software manufacturer's documentation for instructions.

You can download the CSV file for any CSV report you view in Cisco Secure ACS. The procedure below includes steps for doing so.

To view a CSV report, follow these steps:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click the name of the CSV report you want to view.

Result: On the right side of the browser, Cisco Secure ACS lists the current CSV report file name and the file names of any old CSV report files.

Downloaded from www.Manualslib.com manuals search engine

Tip You can configure how Cisco Secure ACS handles old CSV report files. For more information, see the "Configuring a CSV Log" section on page 9-22.

Step 3 Click the CSV report file name whose contents you want to view.

Result: If the CSV report file contains information, the information appears in the display area.

Tip You can sort the table by any column's entries, in either ascending or descending order. Click a column title once to sort the table by that column's entries in ascending order. Click the column a second time to sort the table by that column's entries in descending order.

Tip To check for newer information in the current CSV report, click **Refresh**.

Step 4 If you want to download the CSV log file for the report you are viewing, follow these steps:

a. Click **Download**.

Result: Your browser displays a dialog box for accepting and saving the CSV file.

b. Choose a location to save the CSV file and save the file.

Configuring a CSV Log

This procedure describes how to configure the content of a CSV log. For instructions about enabling or disabling a CSV log, see the "Enabling or Disabling a CSV Log" section on page 9-19.

The logs to which this procedure applies are:

- TACACS+ Accounting
- TACACS+ Administration

Downloaded from www.Manualslib.com manuals search engine

- RADIUS Accounting
- VoIP Accounting
- Failed Attempts
- Passed Authentications

Note The ACS Backup and Restore, RDBMS Synchronization, and Database Replication CSV logs cannot be configured.

You can configure several aspects of a CSV log:

- **Log content—**You can select which data attributes are included in the log.
- **Log generation frequency—**You can determine whether a new log is started after a specific length of time or when the current CSV file reaches a particular size.
- **CSV file location—**You can specify where on the local hard drive Cisco Secure ACS writes the CSV file.
- **CSV file retention—**You can specify how many old CSV files Cisco Secure ACS maintains or set a maximum number of files it is to retain.

To configure a CSV log, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Logging**.

Step 3 Click the name of the CSV log you want to enable.

Result: The CSV *log* Comma-Separated Values File Configuration page appears, where *log* is the name of the CSV log you selected.

The Select Columns To Log table contains two lists, Attributes and Logged Attributes. The attributes in the Logged Attributes list appear on the log selected.

Step 4 To add an attribute to the log, select the attribute in the Attributes list, and then click —> (right arrow button).

Result: The attribute moves to the Logged Attributes list.

Tip Use the vertical scroll bar to find attributes not visible in the list box.

Downloaded from www.Manualslib.com manuals search engine

Step 5 To remove an attribute from the log, select the attribute in the Logged Attributes list, then click <— (left arrow button).

Result: The attribute moves to the Attributes list.

Tip Use the vertical scroll bar to find attributes not visible in the list.

Step 6 To set the attributes in the Logged Attributes list back to the default selections, at the bottom of the browser window, click **Reset Columns**.

Step 7 To generate a new CSV file at a regular interval, select one of the following options:

- **Every day**—Cisco Secure ACS generates a new CSV file at the start of each day.
- **Every week**—Cisco Secure ACS generates a new CSV file at the start of each week.
- **Every month**—Cisco Secure ACS generates a new CSV file at the start of each month.

Step 8 To generate a new CSV file when the current file reaches a specific size, select the **When size is greater than** *x* **KB** option and type the file size threshold, in kilobytes, in the *x* box.

Step 9 To manage which CSV files Cisco Secure ACS keeps, follow these steps:

a. Select the **Manage Directory** check box.

b. To limit the number of CSV files Cisco Secure ACS retains, select the **Keep only the last** *x* **files** option and type the number of files you want Cisco Secure ACS to retain in the *x* box.

c. To limit how old CSV files retained by Cisco Secure ACS can be, select the **Delete files older than** *x* **days** option and type the number of days for which Cisco Secure ACS should retain a CSV file before deleting it.

Step 10 Click **Submit**.

Result: Cisco Secure ACS implements the CSV log configuration that you specified.

Downloaded from www.Manualslib.com manuals search engine

Working with ODBC Logs

This section contains procedures for the following topics:

- Preparing to Use ODBC Logging, page 9-25
- Configuring a System Data Source Name for ODBC Logging, page 9-26
- Configuring a CSV Log, page 9-22

Preparing to Use ODBC Logging

If you plan to use ODBC logging, there are several steps you must complete before you configure an ODBC log.

To prepare to use ODBC logging, follow these steps:

Step 1 Set up the relational database to which you want to export logging data. For more information, refer to your relational database documentation.

Step 2 Set up a system data source name (DSN) on the Cisco Secure ACS server. For instructions, see the "Configuring a System Data Source Name for ODBC Logging" section on page 9-26.

Step 3 Enable ODBC logging in the Cisco Secure ACS HTML interface:

a. In the navigation bar, click **Interface Configuration**.

b. Click **Advanced Options**.

c. Select the **ODBC Logging** check box.

d. Click **Submit**.

Result: Cisco Secure ACS enables the ODBC logging feature. On the Logging page, in the System Configuration section, Cisco Secure ACS displays links for configuring ODBC logs.

Result: You can now configure individual ODBC logs. For instructions, see the "Configuring an ODBC Log" section on page 9-27.

Downloaded from www.Manualslib.com manuals search engine

Configuring a System Data Source Name for ODBC Logging

On the Cisco Secure ACS server, you must create a system DSN for Cisco Secure ACS to communicate with the relational database that is to store your logging data.

To create a system DSN for use with ODBC logging, follow these steps:

Step 1 In Windows Control Panel, double-click **ODBC Data Sources**.

Step 2 In the ODBC Data Source Administrator page, click the **System DSN** tab.

Step 3 Click **Add**.

Step 4 Select the driver you need to use with your new DSN, and then click **Finish**.

Result: A dialog box displays fields requiring information specific to the ODBC driver you selected.

Step 5 Type a descriptive name for the DSN in the Data Source Name box.

Step 6 Complete the other fields required by the ODBC driver you selected. These fields may include information such as the IP address of the server on which the ODBC-compliant relational database runs.

Step 7 Click **OK**.

Step 8 Close the ODBC window and Windows Control Panel.

Result: The System DSN to be used by Cisco Secure ACS for communication with the relational database is created on your Cisco Secure ACS server. The name you assigned to the DSN appears in the Data Source list on each ODBC log configuration page.

Downloaded from www.Manualslib.com manuals search engine

Configuring an ODBC Log

The logs to which this procedure applies are:

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Failed Attempts

Note Before you can configure an ODBC log, you must prepare for ODBC logging. For more information, see the "Preparing to Use ODBC Logging" section on page 9-25.

To configure an ODBC log, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Logging**.

Step 3 Click the name of the ODBC log you want to enable.

Result: The ODBC *log* Configuration page appears, where *log* is the name of the ODBC log you selected.

The Select Columns To Log table contains two lists: Attributes and Logged Attributes. When you first access the ODBC configuration page for a log, the Logged Attributes list contains the default set of attributes. Cisco Secure ACS includes in the log only those attributes that are in the Logged Attributes list.

Step 4 Specify the attributes that you want Cisco Secure ACS to send to the relational database:

a. To add an attribute to the log, select the attribute in the Attributes list, and then click —> (right arrow button).

Result: The attribute moves to the Logged Attributes list.

Tip Use the vertical scroll bar to find attributes not visible in the list box.

Downloaded from www.Manualslib.com manuals search engine

b. To remove an attribute from the log, select the attribute in the Logged Attributes list, and then click <— (left arrow button).

Result: The attribute moves to the Attributes list.

Tip Use the vertical scroll bar to find attributes not visible in the list box.

c. To set the attributes in the Logged Attributes list back to the default selections, click **Reset Columns**.

Step 5 In the ODBC Connection Settings table, follow these steps:

a. From the Data Source list, select the system DSN you created to allow Cisco Secure ACS to send ODBC logging data to your relational database.

b. In the **Username** box, type the username of a user account in your relational database.

Note The user must have sufficient privileges in the relational database to write the ODBC logging data to the appropriate table.

c. In the **Password** box, type the password for the relational database user account you specified in Step B.

d. In the **Table Name** box, type the name of the table to which you want ODBC logging data appended.

Step 6 Click **Submit**.

Result: Cisco Secure ACS saves the log configuration.

Step 7 Click the name of the ODBC log you are configuring.

Result: Cisco Secure ACS displays the ODBC log configuration page again.

Step 8 Click **Show Create Table**.

Result: The right side of the browser displays an SQL create table statement for Microsoft SQL Server. The table name is the name specified in the Table Name box. The column names are the attributes specified in the Logged Attributes list.

Downloaded from www.Manualslib.com manuals search engine

Note The generated SQL is valid for Microsoft SQL Server only. If you are using another relational database, refer to your relational database documentation for information about writing a command to create a table.

Step 9 Using the information provided in the generated SQL, create a table in your relational database for this ODBC log.

Note In order for ODBC logging to work, the table name and the column names must match exactly the names in the generated SQL.

Step 10 Continuing in Cisco Secure ACS, access the configuration page for the ODBC log you are configuring:

a. In the navigation bar, click **System Configuration**.

b. Click **Logging**.

c. Click the name of the ODBC log you are configuring.

Result: The ODBC *log* Configuration page appears, where *log* is the name of the ODBC log you selected.

Step 11 Select the **Log to ODBC** *log* **report** check box, where *log* is the name of the ODBC log you selected.

Step 12 Click **Submit**.

Result: Cisco Secure ACS begins sending logging data to the relational database table specified, using the system DSN you configured.

Remote Logging

This section discusses remote logging capabilities of Cisco Secure ACS. It contains the following topics:

- About Remote Logging, page 9-30
- Remote Logging Options, page 9-31
- Configuring a Central Logging Server, page 9-31

Downloaded from www.Manualslib.com manuals search engine

- Enabling and Configuring Remote Logging, page 9-32
- Disabling Remote Logging, page 9-33

About Remote Logging

The Remote Logging feature enables you to centralize accounting logs generated by multiple Cisco Secure ACS servers. You can configure each Cisco Secure ACS to point to a single Cisco Secure ACS that is to be used as the logging server. The logging Cisco Secure ACS server can still perform its AAA duties, but it also is the repository for accounting logs it receives. For more information about Cisco Secure ACS accounting logs, see the "Accounting Logs" section on page 9-4.

The Remote Logging feature sends accounting data received from AAA clients by the local Cisco Secure ACS server directly to the CSLOG service on the remote logging server, where the accounting data is written to the logs. The logging server generates the accounting logs in the formats it is configured to use—CSV and ODBC—regardless of the local logging configuration on the servers sending the data to the logging server.

Note The Remote Logging feature does not affect the forwarding of accounting data for proxied authentication requests. Cisco Secure ACS only applies Remote Logging settings to accounting data for sessions authenticated by proxy when accounting data for sessions authenticated by proxy is logged locally. For more information about proxied authentication requests and accounting data for sessions authenticated by proxy, see the "Proxy Distribution Table Configuration" section on page 4-25.

Downloaded from www.Manualslib.com manuals search engine

Remote Logging Options

Cisco Secure ACS provides the remote logging options listed below. These options appear on the Remote Logging page, available from the Logging page in the System Configuration section.

- **Do not Log Remotely—**Cisco Secure ACS writes accounting data of locally authenticated sessions only to the local logs that are enabled.
- **Log To All Selected Hosts—**Cisco Secure ACS sends accounting data for locally authenticated sessions to all the AAA servers in the Log To list.
- **Log to Subsequent Selected Hosts on Failure—**Cisco Secure ACS sends accounting data for locally authenticated sessions to the first Cisco Secure ACS server in the Log To list that is operational. This behavior enables you to configure one or more backup central logging servers so that no accounting data is lost if the first central logging server fails or is otherwise unavailable to the local Cisco Secure ACS server.
- **Log Servers—**This list represents the AAA servers configured in the AAA Servers table in Network Configuration to which the Cisco Secure ACS server *does not* send accounting data for locally authenticated sessions.
- **Log To—**This list represents the AAA servers configured in the AAA Servers table in Network Configuration to which the Cisco Secure ACS server *does* send accounting data for locally authenticated sessions.

Configuring a Central Logging Server

A central logging server is a Cisco Secure ACS server that is to receive accounting data from Cisco Secure ACS servers configured to do remote logging. Configuring a central logging server consists entirely of making sure that all Cisco Secure ACS servers that are to send their accounting data are defined in the central logging server's AAA Servers table.

For each Cisco Secure ACS server that the central logging server is to log watchdog and update packets, be sure that the Log Update/Watchdog Packets from this remote AAA Server check box is selected in that server's entry in the central logging server's AAA Servers table.

For more information about the AAA Servers table, see the "AAA Server Configuration" section on page 4-15.

Downloaded from www.Manualslib.com manuals search engine

Enabling and Configuring Remote Logging

Note Before configuring the Remote Logging feature on a Cisco Secure ACS server, make sure that you have configured your central logging server. For more information, see the "Configuring a Central Logging Server" section on page 9-31.

To enable and configure remote logging, follow these steps:

Step 1 To enable the Remote Logging feature in the HTML interface, follow these steps:

a. Click **Interface Configuration**.

b. Click **Advanced Options**.

c. Select the **Remote Logging** check box.

d. Click **Submit**.

Result: Cisco Secure ACS displays the Remote Logging link on the Logging page in the System Configuration section.

Step 2 Click **System Configuration**.

Step 3 Click **Logging**.

Step 4 Click **Remote Logging**.

Step 5 Select the applicable remote logging option:

a. To disable remote logging, select the **Do not Log Remotely** option.

b. To send this Cisco Secure ACS server's accounting information to more than one Cisco Secure ACS server, select the **Log to All Selected Hosts** option.

c. To send this Cisco Secure ACS server's accounting information to a single Cisco Secure ACS server, select the **Log to Subsequent Selected Hosts on Failure** option.

Note Use the Log to Subsequent Selected Hosts on Failure option when you want to configure Cisco Secure ACS to send accounting data to a second remote Cisco Secure ACS server if the first server fails.

Downloaded from www.Manualslib.com manuals search engine

Step 6 For each remote Cisco Secure ACS server you want to have in the Log To list, follow these steps:

a. In the Log Servers list, select the name of a Cisco Secure ACS server to which you want to send accounting data for locally authenticated sessions.

Note The Cisco Secure ACS servers available in the Log Servers list is determined by the AAA Servers table in Network Configuration. For more information about the AAA Servers table, see the "AAA Server Configuration" section on page 4-15.

b. Click —> (right arrow button) to move the selected Cisco Secure ACS server to the Log To list.

Step 7 To assign an order to the servers in the Log To list, click **Up** and **Down** to move selected Cisco Secure ACS servers until you have created the order you need.

Note If the Log to Subsequent Selected Hosts on Failure option is selected, Cisco Secure ACS logs to the first accessible Cisco Secure ACS server Log To list.

Step 8 Click **Submit**.

Result: Cisco Secure ACS saves and implements the remote logging configuration you specified.

Disabling Remote Logging

You can prevent a Cisco Secure ACS server from sending its accounting information to a central logging Cisco Secure ACS server by disabling the Remote Logging feature.

To disable remote logging, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Logging**.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Click **Remote Logging**.

Step 4 Select the **Do not Log Remotely** option.

Step 5 Click **Submit**.

Result: This Cisco Secure ACS server no longer sends its accounting information for locally authenticated sessions to remote logging servers.

Service Logs

The service logs may be considered diagnostic logs and are used for troubleshooting or debugging purposes only. These logs are not intended for general use by Cisco Secure ACS administrators; instead, they are mainly sources of information for Cisco support personnel. Service logs contain a record of all Cisco Secure ACS service actions and activities. Cisco Secure ACS generates these logs whenever you log in to Windows NT/2000 and the services are started, whether or not the administrative interface is started, and whether or not you are using the service. For example, RADIUS service logs are created even if you are not using the RADIUS protocol in your network.

For more information about Cisco Secure ACS services, see Appendix H, "Cisco Secure ACS Internal Architecture."

Services Logged

Cisco Secure ACS generates logs for the following services:

- CSAdmin
- CSAuth
- CSDBSync
- CSLog
- CSMon
- CSRadius
- CSTacacs

Downloaded from www.Manualslib.com manuals search engine

These files are located in the `\Logs` subdirectory of the applicable service's directory. For example, the following is the default directory for the CiscoSecure authentication service:

```
c:\Program Files\CiscoSecure ACS v2.6\CSAuth\Logs
```

The most recent debug log is named as follows:

SERVICE`.log`

where *SERVICE* is the name of the applicable service.

Older debug logs are named with the year, month, and date they were created. For example, a file created on July 13, 1999, would be named as follows:

SERVICE `1999-07-13.log`

where *SERVICE* is the name of the applicable service.

If you selected the Day/Month/Year format, the file would be named as follows:

SERVICE `13-07-1999.log`

Configuring Service Logs

You can configure how Cisco Secure ACS generates and manages the service log file. The options for configuring the service log file are listed below.

- **Level of detail—**You can set the service log file to contain one of three levels of detail:
  - **None—**No log file is generated.
  - **Low—**Only start and stop actions are logged.
  - **Full—**All services actions are logged.
- **Generate new file—**You can control how often a new service log file is created:
  - **Every Day—**Cisco Secure ACS generates a new log file at 12:01 A.M. local time every day.
  - **Every Week—**Cisco Secure ACS generates a new log file at 12:01 A.M. local time every Sunday.

Downloaded from www.Manualslib.com manuals search engine

  - **Every Month—**Cisco Secure ACS generates a new log file at 12:01 A.M. on the first day of every month.
  - **When Size is Greater than *x* KB**—Cisco Secure ACS generates a new log file after the current service log file reaches the size specified, in kilobytes, by *x*.

- **Manage Directory—**You can control how long services log files are kept:
  - **Keep only the last *x* files**—Cisco Secure ACS retains, at most, the number of files specified by *x*.
  - **Delete files older than *x* days**—Cisco Secure ACS retains only those service logs that are not older than the number of days specified by *x*.

To configure how Cisco Secure ACS generates and manages the service log file, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Service Control**.

Result: The status of the services appears in the CiscoSecure ACS on *hostname* table, where *hostname* is the name of the Cisco Secure ACS server.

Step 3 To disable the service log file, under Level of detail, select the **None** option.

Result: After you click Restart, Cisco Secure ACS does not generate new service logs file.

Step 4 To configure how often Cisco Secure ACS creates a service log file, select one of the options under Generate New File.

Note Settings under Generate New File have no effect if you selected None under Level of detail.

Downloaded from www.Manualslib.com manuals search engine

Step 5 To manage which service log files Cisco Secure ACS keeps, follow these steps:

a. Select the **Manage Directory** check box.

b. To limit the number of service log files Cisco Secure ACS retains, select the **Keep only the last** *x* **files** option and in the *x* box type the number of files you want Cisco Secure ACS to retain.

c. To limit how old service log files retained by Cisco Secure ACS can be, select the **Delete files older than** *x* **days** option and in the *x* box type the number of days for which Cisco Secure ACS should retain a service log file before deleting it.

Step 6 Click **Restart**.

Result: Cisco Secure ACS restarts its services and implements the service log settings you specified.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 10

Setting Up and Managing Administrators and Policy

This chapter addresses the Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) features found in the Administration Control section of the HTML interface. It contains the following sections:

- Administrator Accounts, page 10-1
- Access Policy, page 10-10
- Session Policy, page 10-13
- Audit Policy, page 10-16

Administrator Accounts

To access the Cisco Secure ACS HTML interface from a browser run elsewhere than on the Cisco Secure ACS server itself, you must log in to Cisco Secure ACS using an administrative account. If your Cisco Secure ACS is so configured, you may need to log in to Cisco Secure ACS even on the Cisco Secure ACS server. For more information about automatic local logins, see the "Session Policy" section on page 10-13.

Downloaded from www.Manualslib.com manuals search engine

Note Cisco Secure ACS administrator accounts have no correlation with Cisco Secure ACS user accounts or username/password authentication. Cisco Secure ACS stores accounts created for authentication of network service requests and those created for Cisco Secure ACS administrative access in separate internal databases.

This section contains the following topics:

- Administrator Privileges, page 10-2
- Adding an Administrator Account, page 10-6
- Editing an Administrator Account, page 10-7
- Deleting an Administrator Account, page 10-9

Administrator Privileges

You can grant appropriate privileges to each Cisco Secure ACS administrator by assigning privileges on an administrator-by-administrator basis. You control privileges by selecting the options in the Administrator Privileges table on the Add Administrator or Edit Administrator pages. These options are listed below:

- **User and Group Setup—**Contains the following privilege options for the User Setup and Group Setup sections of the HTML interface:
  - **Add/Edit users in these groups—**Enables the administrator to add or edit users and to assign users to the groups in the Editable groups list.
  - **Setup of these groups—**Enables the administrator to edit the settings for the groups in the Editable groups list.
  - **Available Groups—**Lists the user groups for which the administrator *does not* have edit privileges and to which the administrator *cannot* add users.
  - **Editable Groups—**Lists the user groups for which the administrator *does* have edit privileges to which the administrator account *can* add users.

Downloaded from www.Manualslib.com manuals search engine

- **Shared Profile Components—**Contains the following privilege options for the Shared Profile Components section of the HTML interface:
  - **Network Access Restriction Sets—**Allows the administrator full access to the Network Access Restriction Sets feature.
  - **Downloadable ACLs—**Allows the administrator full access to the Downloadable PIX ACLs feature.
  - **Create New Device Command Set Type—**Allows the administrator's account to be used as valid credentials by another Cisco application for adding new device command set types.
  - **Shell Command Authorization Sets—**Allows the administrator full access to the Shell Command Authorization Sets feature.
  - **PIX Command Authorization Sets—**Allows the administrator full access to the PIX Command Authorization Sets feature.

Note Additional command authorization set privilege options may appear, if other Cisco network management applications, such as CiscoWorks2000, have updated the configuration of Cisco Secure ACS.

- **Network Configuration—**Allows the administrator full access to the features in the Network Configuration section of the HTML interface.
- **System Configuration...—**Contains the privilege options for the features found in the System Configuration section of the HTML interface. For each of the following features, enabling the option allows the administrator full access to the feature.
  - **Service Control—**For more information about this feature, see the "Service Control" section on page 8-2.
  - **Date/Time Format Control—**For more information about this feature, see the "Date Format Control" section on page 8-3.
  - **Logging Control—**For more information about this feature, see the "Logging" section on page 8-3.
  - **Password Validation—**For more information about this feature, see the "Password Validation" section on page 8-4.
  - **DB Replication—**For more information about this feature, see the "CiscoSecure Database Replication" section on page 8-6.

Downloaded from www.Manualslib.com manuals search engine

  - **RDBMS Synchronization—**For more information about this feature, see the "RDBMS Synchronization" section on page 8-24.
  - **IP Pool Address Recovery—**For more information about this feature, see the "IP Pools Address Recovery" section on page 8-59.
  - **IP Pool Server Configuration—**For more information about this feature, see the "IP Pools Server" section on page 8-52.
  - **ACS Backup—**For more information about this feature, see the "Cisco Secure ACS Backup" section on page 8-40.
  - **ACS Restore—**For more information about this feature, see the "Cisco Secure ACS System Restore" section on page 8-45.
  - **ACS Service Management—**For more information about this feature, see the "Cisco Secure ACS Active Service Management" section on page 8-48.
  - **VoIP Accounting Configuration—**For more information about this feature, see the "VoIP Accounting Configuration" section on page 8-60.
  - **ACS Certificate Configuration—**For more information about this feature, see the "Cisco Secure ACS Certificate Setup" section on page 8-61.
  - **Certification Authority Configuration—**For more information about this feature, see the "Certification Authority Setup" section on page 8-70.

- **Interface Configuration—**Allows the administrator full access to the features in the Interface Configuration section of the HTML interface.
- **Administration Control—**Allows the administrator full access to the features in the Administration Control section of the HTML interface.
- **External User Databases—**Allows the administrator full access to the features in the External User Databases section of the HTML interface.

Downloaded from www.Manualslib.com manuals search engine

- **Reports & Activity**—Contains the privilege options for the reports and features found in the Reports and Activity section of the HTML interface. For each of the following features, enabling the option allows the administrator full access to the feature.
  - **TACACS+ Accounting—**For more information about this report, see the "TACACS+ Accounting Log" section on page 9-5.
  - **TACACS+ Administration—**For more information about this report, see the "TACACS+ Administration Log" section on page 9-6.
  - **RADIUS Accounting—**For more information about this report, see the "RADIUS Accounting Log" section on page 9-7.
  - **VoIP Accounting—**For more information about this report, see the "VoIP Accounting Log" section on page 9-8.
  - **Passed Authentications—**For more information about this report, see the "Passed Authentications Log" section on page 9-10.
  - **Failed Attempts—**For more information about this report, see the "Failed Attempts Log" section on page 9-9.
  - **Logged-in Users—**For more information about this report, see the "Logged-In Users Report" section on page 9-11.
  - **Purge of Logged-in Users—**For more information about this feature, see the "Deleting Logged-in Users" section on page 9-12.
  - **Disabled Accounts—**For more information about this report, see the "Disabled Accounts Report" section on page 9-14.
  - **ACS Backup and Restore—**For more information about this report, see the "ACS Backup and Restore Log" section on page 9-15.
  - **DB Replication—**For more information about this report, see the "Database Replication Log" section on page 9-16.
  - **RDBMS Synchronization—**For more information about this report, see the "RDBMS Synchronization Log" section on page 9-16.
  - **Administration Audit—**For more information about this report, see the "Administration Audit Log" section on page 9-17.
  - **ACS Service Monitor—**For more information about this report, see the "ACS Service Monitoring Log" section on page 9-18.

Downloaded from www.Manualslib.com manuals search engine

Adding an Administrator Account

You can add Cisco Secure ACS administrator accounts to allow remote access to the HTML interface. If, on the Session Policy page, the Allow automatic local login check box is *not* selected, Cisco Secure ACS requires that you log in using an administrative account for administrative sessions local to the Cisco Secure ACS server, too.

For information about the administrative privilege options, see the "Administrator Privileges" section on page 10-2.

To add a Cisco Secure ACS administrator account, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Step 2 Click **Add Administrator**.

Result: The Add Administrator page appears.

Step 3 Complete the boxes in the Administrator Details table:

a. In the **Administrator Name** box, type the login name for the new Cisco Secure ACS administrator account.

Note The Administrator Name can contain special characters, including spaces.

b. In the **Password** box, type the password for the new Cisco Secure ACS administrator account.

c. In the **Confirm Password** box, type the password a second time.

Step 4 To select all privileges, including user group editing privileges for all user groups, click **Grant All**.

Result: All privileges options are selected. All user groups move to the Editable groups list.

Tip To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

Downloaded from www.Manualslib.com manuals search engine

Step 5 To grant user and user group editing privileges, follow these steps:

a. Select the desired check boxes under User & Group Setup.

b. To move a user group to the Editable groups list, select the group in the Available groups list, and then click —> (right arrow button).

Result: The selected group moves to the Editable groups list.

c. To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click <— (left arrow button).

Result: The selected group moves to the Available groups list.

d. To move all user groups to the Editable groups list, click >>.

Result: The user groups in the Available groups list move to the Editable groups list.

e. To remove all user groups from the Editable groups list, click <<.

Result: The user groups in the Editable groups list move to the Available groups list.

Step 6 To grant any of the remaining privilege options, in the Administrator Privileges table, select the applicable check boxes.

Step 7 Click **Submit**.

Result: Cisco Secure ACS saves the new administrator account. The new account appears in the list of administrator accounts on the Administration Control page.

Editing an Administrator Account

You can edit a Cisco Secure ACS administrator account to change the privileges granted to the administrator. You can effectively disable an administrator account by revoking all privileges.

Downloaded from www.Manualslib.com manuals search engine

Note You cannot change the name of an administrator account; however, you can delete an administrator account and then create an account with the new name. For information about deleting an administrator account, see the "Deleting an Administrator Account" section on page 10-9. For information about creating an administrator account, see the "Adding an Administrator Account" section on page 10-6.

For information about the administrative privilege options, see the "Administrator Privileges" section on page 10-2.

To edit Cisco Secure ACS administrator account privileges, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 Click the name of the administrator account whose privileges you want to edit.

Result: The Edit Administrator *name* page appears, where *name* is the name of the administrator account you selected in Step 2.

Step 3 To change the administrator password, follow these steps:

a. In the **Password** box, double-click the asterisks, and then type the new password for the administrator.

Result: The new password replaces the existing, masked password.

b. In the **Confirm Password** box, double-click the asterisks, and then type the new administrator password a second time.

Step 4 To select all privileges, including user group editing privileges for all user groups, click **Grant All**.

Result: All privileges options are selected. All user groups move to the Editable groups list.

Step 5 To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

Result: All privileges options are cleared. All user groups move to the Available groups list.

Downloaded from www.Manualslib.com manuals search engine

Step 6 To grant user and user group editing privileges, follow these steps:

a. Under User & Group Setup, select the applicable check boxes.

b. To move all user groups to the Editable groups list, click >>.

Result: The user groups in the Available groups list move to the Editable groups list.

c. To move a user group to the Editable groups list, select the group in the Available groups list, and then click —> (right arrow button).

Result: The selected group moves to the Editable groups list.

d. To remove all user groups from the Editable groups list, click <<.

Result: The user groups in the Editable groups list move to the Available groups list.

e. To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click <— (left arrow button).

Result: The selected group moves to the Available groups list.

Step 7 To grant any remaining privilege options, select the applicable check boxes in the Administrator Privileges table.

Step 8 To revoke any remaining privilege options, clear the applicable check boxes in the Administrator Privileges table.

Step 9 Click **Submit**.

Result: Cisco Secure ACS saves the changes to the administrator account.

Deleting an Administrator Account

You can delete a Cisco Secure ACS administrator account when you no longer need it. We recommend deleting any unused administrator accounts.

To delete a Cisco Secure ACS administrator account, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Downloaded from www.Manualslib.com manuals search engine

Step 2 In the Administrators table, click the name of the administrator account that you want to delete.

Result: The Edit Administrator *name* page appears, where *name* is the name of the administrator account you selected in Step 2.

Step 3 Click **Delete**.

Result: Cisco Secure ACS displays a confirmation dialog box.

Step 4 Click **OK**.

Result: Cisco Secure ACS deletes the administrator account. The Administrators table on the Administration Control page no longer lists administrator account that you deleted.

Access Policy

The Access Policy feature affects access to remote Cisco Secure ACS administration sessions. You can limit remote administrator access by IP address and by the TCP port range used for administrative sessions. This section contains the following topics:

- Access Policy Options, page 10-10
- Setting Up Session Policy, page 10-14

Access Policy Options

You can configure the following options on the Access Policy Setup page:

- **IP Address Filtering—**Contains the following IP address filtering options:
  - **Allow all IP addresses to connect—**Allow remote access to the HTML interface from any IP address.
  - **Allow only listed IP addresses to connect—**Allow remote access to the HTML interface only from IP addresses *inside* the address range(s) specified in the IP Address Ranges table.

Downloaded from www.Manualslib.com manuals search engine

  - **Reject connections from listed IP addresses—**Allow remote access to the HTML interface only from IP addresses *outside* the address range(s) specified in the IP Address Ranges table.

- **IP Address Ranges—**The IP Address Ranges table contains ten rows for configuring IP address ranges. The ranges are always inclusive; that is, the range includes the start and end IP addresses. The IP addresses entered to define a range must differ only in the last octet (Class C format).

  The IP Address Ranges table contains one column of each of the following boxes:

  - **Start IP Address—**Defines the lowest IP address of the range specified in the current row.
  - **End IP Address—**Defines the highest IP address of the range specified in the current row.

- **HTTP Port Allocation—**Contains the following options for configuring TCP ports used for remote access to the HTML interface.

  - **Allow any TCP ports to be used for Administration HTTP Access—**Allow the ports used by administrative HTTP sessions to include the full range of TCP ports.
  - **Restrict Administration Sessions to the following port range From Port** *x* **to Port** *y*—Restrict the ports used by administrative HTTP sessions to the range specified in the *x* and *y* boxes, inclusive. The size of the range specified determines the maximum number of concurrent administrative sessions.

    A firewall configured to permit HTTP traffic over the Cisco Secure ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port a remote web browser must access to initiate an administrative session.

Note We do not recommend allowing administration of Cisco Secure ACS from outside a firewall. If you do choose to allow remote access to the HTML interface from outside a firewall, keep the HTTP port range as narrow as possible. This can help prevent accidental discovery of an active administrative port by unauthorized users. An unauthorized user would have to impersonate, or "spoof," the IP address of a legitimate remote host to make use of the active administrative session HTTP port.

Downloaded from www.Manualslib.com manuals search engine

Setting Up Access Policy

For information about access policy options, see the "Access Policy Options" section on page 10-10.

To set up Cisco Secure ACS Access Policy, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 Click **Access Policy**.

Result: The Access Policy Setup page appears.

Step 3 To allow remote access to the HTML interface from any IP address, in the IP Address Filtering table, select the **Allow all IP addresses to connect** option.

Step 4 To allow remote access to the HTML interface only from IP addresses *within* a range or ranges of IP addresses, follow these steps:

a. In the IP Address Filtering table, select the **Allow only listed IP addresses to connect** option.

b. For each IP address range from within which you want to allow remote access to the HTML interface, complete one row of the IP Address Ranges table. In the Start IP Address box, type the lowest IP address in the range. In the End IP Address box, type the highest IP address in the range.

Step 5 To allow remote access to the HTML interface only from IP addresses *outside* a range or ranges of IP addresses, follow these steps:

a. In the IP Address Filtering table, select the **Reject connections from listed IP addresses** option.

b. For each IP address range from outside of which you want to allow remote access to the HTML interface, complete one row of the IP Address Ranges table. Type the lowest IP address in the range in the Start IP Address box. Type the highest IP address in the range in the End IP Address box.

Step 6 To allow Cisco Secure ACS to use any valid TCP port for administrative sessions, either local or remote, select the **Allow any TCP ports to be used for Administration HTTP Access** option.

Downloaded from www.Manualslib.com manuals search engine

Step 7 To allow Cisco Secure ACS to use only a specified range of TCP ports for administrative sessions, follow these steps:

a. Select the **Restrict Administration Sessions to the following port range From Port** *x* **to Port** *y* option.

b. In the *y* box type the highest TCP port in the range.

c. In the *x* box type the lowest TCP port in the range.

Step 8 Click **Submit**.

Result: Cisco Secure ACS saves and begins enforcing the access policy settings.

Session Policy

The Session Policy feature controls various aspects of Cisco Secure ACS administrative sessions. This section contains the following topics:

- Session Policy Options, page 10-13
- Setting Up Session Policy, page 10-14

Session Policy Options

You can configure the following options on the Session Policy Setup page:

- **Session idle timeout (minutes)—**Defines the time in minutes that an administrative session, local or remote, must remain idle before Cisco Secure ACS terminates the connection. This parameter applies to the Cisco Secure ACS administrative session in the browser only. It does not apply to an administrator's dial-up session.

  An administrator whose administrative session is terminated receives a dialog box asking whether or not the administrator wants to continue. If the administrator chooses to continue, Cisco Secure ACS starts a new administrative session.

Downloaded from www.Manualslib.com manuals search engine

- **Allow Automatic Local Login—**Enables administrators to start an administrative session without logging in if they are using a browser on the Cisco Secure ACS server. Local administrative sessions with automatic local login are recorded in the Administrative Audit report with the administrator name “local_login”.

Note If there are no administrator accounts defined, no administrator name and password is required to access Cisco Secure ACS locally. This prevents you from accidentally locking yourself out of Cisco Secure ACS.

- **Respond to Invalid IP Address Connections—**Enables an error message in response to attempts to start a remote administrative session using an IP address that is invalid according to the IP address ranges configured in Access Policy. Disabling this option can help prevent unauthorized users from discovering your Cisco Secure ACS server.
- **Lock out Administrator after** *x* **successive failed attempts**—Enables Cisco Secure ACS to lock out an administrator after the number of successive failed login attempts specified in the *x* box. A value of 0 (zero) in the x box allows unlimited successive administrative login failures. If this check box is selected, the x box cannot be set to zero.

Setting Up Session Policy

For information about session policy options, see “Session Policy Options” section on page 10-13.

To setup Cisco Secure ACS Session Policy, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 Click **Session Policy**.

Result: The Session Policy Setup page appears.

Step 3 To define the number of minutes of inactivity after which Cisco Secure ACS ends an administrative session, in the Session idle timeout (minutes) box, type the number of minutes.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Set the automatic local login policy:

a. To allow administrators to login to Cisco Secure ACS locally without using their administrator names and passwords, select the **Allow Automatic Local Login** check box.

b. To require administrators to login to Cisco Secure ACS locally using their administrator names and passwords, clear the **Allow Automatic Local Login** check box.

Step 5 Set the invalid IP address response policy:

a. To configure Cisco Secure ACS to respond with a message when an administrative session is requested from an invalid IP address, select the **Respond to invalid IP address connections** check box.

b. To configure Cisco Secure ACS to send no message when an administrative session is requested from an invalid IP address, clear the **Respond to invalid IP address connections** check box.

Step 6 Set the failed administrative login attempts policy:

a. To enable Cisco Secure ACS to lockout an administrator after a number of successive failed administrative login attempts, select the **Lock out Administrator after** *x* **successive failed attempts** check box.

b. In the *x* box, type the number of successive failed login attempts after which Cisco Secure ACS locks out an administrator. To allow unlimited failed administrative login attempts, type **0** (zero).

Note If the Lock out Administrator after *x* successive failed attempts check box is selected, the *x* box cannot be set to zero.

Step 7 Click **Submit**.

Result: Cisco Secure ACS saves and begins enforcing the session policy settings you made.

Downloaded from www.Manualslib.com manuals search engine

Audit Policy

The Audit Policy feature controls the generation of the Administrative Audit log.

For more information about enabling, viewing, or configuring the Administrative Audit log, see the "Administration Audit Log" section on page 9-17.

Downloaded from www.Manualslib.com manuals search engine

Working with User Databases

Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) authenticates users against one of several possible databases, including its internal database. You can configure Cisco Secure ACS to authenticate users with more than one type of database. This flexibility enables you to use user accounts data collected in different locations without having to explicitly import the users from each external user database into the CiscoSecure user database. It also enables you to apply different databases to different types of users, depending on the security requirements associated with user authorizations on your network. For example, a common configuration is to use a Windows 2000/NT user database for standard network users and a token server for network administrators.

This chapter contains the following sections:

- CiscoSecure User Database, page 11-2
- About External User Databases, page 11-4
- Windows NT/2000 User Database, page 11-6
- Generic LDAP, page 11-14
- Novell NDS Database, page 11-24
- ODBC Database, page 11-30
- LEAP Proxy RADIUS Server Database, page 11-44
- Token Server User Databases, page 11-47
- Deleting an External User Database Configuration, page 11-58

For information about the Unknown User Policy and group mapping features, see Chapter 12, “Administering External User Databases.”

Downloaded from www.Manualslib.com manuals search engine

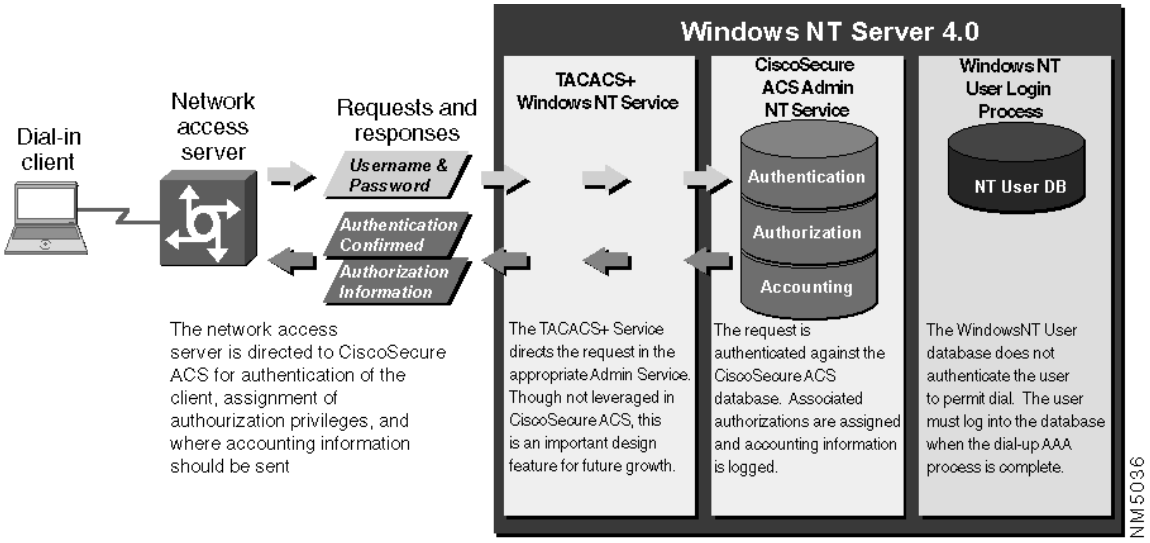
CiscoSecure User Database

The CiscoSecure user database is the database internal to Cisco Secure ACS. The CiscoSecure user database draws information from a number of data sources, including a memory-mapped, hash-indexed file, VarsDB.MDB (in Microsoft Jet database format), and the Windows NT/2000 Registry. The memory-mapped, hash-indexed file uses an index and tree structure, so searches can occur logarithmically rather than linearly, thus yielding very fast lookup times. This enables the CiscoSecure user database to authenticate users quickly. See Figure 11-1 on page 11-3.

Unless you have configured Cisco Secure ACS to authenticate users with an external user database, Cisco Secure ACS uses usernames and passwords in the CiscoSecure user database during authentication. If you have configured the Unknown User policy, Cisco Secure ACS does not rely on a username and password in the CiscoSecure user database for authentication. For more information about the Unknown User Policy feature, see the "Unknown User Processing" section on page 12-1. If you have configured specific user accounts to use an external user database to authenticate those users, Cisco Secure ACS uses information from the specified external user database to perform authentication. For more information about specifying an external user database for authentication of a user, see the "Adding a Basic User Account" section on page 7-5.

Downloaded from www.Manualslib.com manuals search engine

Figure 11-1 Using the CiscoSecure User Database for Authentication


Windows NT Server 4.0
Dial-in client
Network access server
Requests and responses
Username & Password
Authentication Confirmed
Authorization Information
TACACS+ Windows NT Service
CiscoSecure ACS Admin NT Service
Windows NT User Login Process
Authentication
Authorization
Accounting
NT User DB
The network access server is directed to CiscoSecure ACS for authentication of the client, assignment of authourization privileges, and where accounting information should be sent
The TACACS+ Service directs the request in the appropriate Admin Service. Though not leveraged in CiscoSecure ACS, this is an important design feature for future growth.
The request is authenticated against the CiscoSecure ACS database. Associated authorizations are assigned and accounting information is logged.
The WindowsNT User database does not authenticate the user to permit dial. The user must log into the database when the dial-up AAA process is complete.
NM5036

There are five ways to create user accounts in the CiscoSecure user database:

- Using the Cisco Secure ACS HTML interface (see the "Adding a Basic User Account" section on page 7-5).
- Using the Database Replication feature (see the "CiscoSecure Database Replication" section on page 8-6).
- Using the Database Import utility, `CSUtil.exe` (see the "Cisco Secure ACS Command-Line Database Utility" section on page E-1.)
- Using the RDBMS Synchronization feature (see the "RDBMS Synchronization" section on page 8-24).
- Using the Unknown User Policy feature (see the "Administering External User Databases" section on page 12-1).

The CiscoSecure user database also is crucial for the authorization process. Regardless of whether a user is authenticated by the internal user database or by an external user database, Cisco Secure ACS authorizes network services for users based upon group membership and specific user settings found in the CiscoSecure user database. Thus, all users authenticated by Cisco Secure ACS, even those whose authentication is performed with an external user database, have an account in the CiscoSecure user database. As always, user settings override group settings.

Downloaded from www.Manualslib.com manuals search engine

If you implement an external user database, Cisco Secure ACS offers two powerful features that you must configure. The first feature is the Unknown User Policy. This feature automates the creation of user accounts in the CiscoSecure user database for users authenticated by an external user database. The other feature is Cisco Secure ACS user group mappings for users authenticated by external user databases. For information on these features, see Chapter 12, "Administering External User Databases."

The CiscoSecure user database supports authentication for PAP, CHAP, MS-CHAP, ARAP, LEAP, and ASCII passwords. It also supports the certificate-based EAP-TLS authentication protocol.

About External User Databases

You can configure Cisco Secure ACS to forward authentication of users to one external user database or more. Support for external user databases means that Cisco Secure ACS does not require that you create duplicate user entries in the CiscoSecure user database. Users can be authenticated using the following databases.

- Windows NT/2000 User Database
- Generic LDAP
- Novell NetWare Directory Services (NDS)
- Open Database Connectivity (ODBC)-compliant relational databases
- LEAP Proxy RADIUS servers
- AXENT token servers
- SafeWord token servers
- RSA SecureID token servers
- RADIUS-based token servers, including:
  - ActivCard token servers
  - CRYPTOCard token servers
  - Vasco token servers
  - Generic RADIUS token servers

Downloaded from www.Manualslib.com manuals search engine

Regardless of which database is used to authenticate users, the CiscoSecure user database, internal to Cisco Secure ACS, is used to authorize requested network services.

For Cisco Secure ACS to interact with an external user database, Cisco Secure ACS requires an API for third-party authentication source. The Cisco Secure ACS communicates with the external user database using the API. For Windows NT/2000, Generic LDAP, and Novell NDS authentication, the program interface for the external authentication is local to the Cisco Secure ACS system and is provided by the local operating system. In these cases, no further components are required.

In the case of ODBC authentication sources, in addition to the Windows ODBC interface, the third-party ODBC driver must be installed on the Cisco Secure ACS server.

To communicate with each traditional token server, you must have software components provided by the OTP vendors installed, in addition to the Cisco Secure ACS components. You must also specify in User Setup that a token card server is to be used.

For RADIUS-based token servers, such as ActivCard, CRYPTOCard, and Vasco, the standard RADIUS interface serves as the third-party API.

Authenticating with External User Databases

Authenticating users with an external user database requires more than configuring Cisco Secure ACS to communicate with an external user database. Performing one of the configuration procedures for an external database that are provided in this chapter does not on its own instruct Cisco Secure ACS to authenticate any users with that database.

Downloaded from www.Manualslib.com manuals search engine

After you have configured Cisco Secure ACS to communicate with an external user database, you can configure Cisco Secure ACS to authenticate users with the external user database in one of two ways:

- **By Specific User Assignment—**You can configure Cisco Secure ACS to authenticate specific users with an external user database. To do this, the user must exist in the CiscoSecure user database and the Password Authentication list in User Setup must be set to the external user database that Cisco Secure ACS is to use to authenticate the user.

  While setting the Password Authentication for every user account is time consuming, this method of determining which users are authenticated with an external user database is secure because it requires explicit definition of who is to authenticate using the external user database. In addition, the users may be placed in the desired Cisco Secure ACS group and thereby receive the applicable access profile.

- **By Unknown User Policy—**You can configure Cisco Secure ACS to attempt authentication of users not found in the CiscoSecure user database by using an external user database. Users do not need to be defined in the CiscoSecure user database for this method. For more information about the Unknown User Policy, see the "Unknown User Processing" section on page 12-1.

You can also configure Cisco Secure ACS with both methods above; these two methods are not mutually exclusive.

Windows NT/2000 User Database

Cisco Secure ACS supports PAP and MS-CHAP authentication with Windows NT 4.0 Security Accounts Manager (SAM) database or a Windows 2000 Active Directory database. Cisco Secure ACS supports EAP-TLS authentication with a Windows 2000 Active Directory database. You can configure Cisco Secure ACS to authenticate usernames and passwords against those already in a Windows NT/2000 user database. In organizations in which a substantial Windows NT/2000 user database already exists, Cisco Secure ACS can leverage the work already invested in building the database without any additional input. This eliminates the need for separate databases.

Downloaded from www.Manualslib.com manuals search engine

This section contains the following topics:

- The Cisco Secure ACS Authentication Process with Windows NT/2000 User Databases, page 11-7
- Trust Relationships, page 11-8
- Windows Dial-up Networking Clients, page 11-9
- Windows NT/2000 Authentication, page 11-10
- User-Changeable Passwords with Windows NT/2000 User Databases, page 11-12
- Preparing Users for Authenticating with Windows NT/2000, page 11-12
- Configuring a Windows NT/2000 External User Database, page 11-13

The Cisco Secure ACS Authentication Process with Windows NT/2000 User Databases

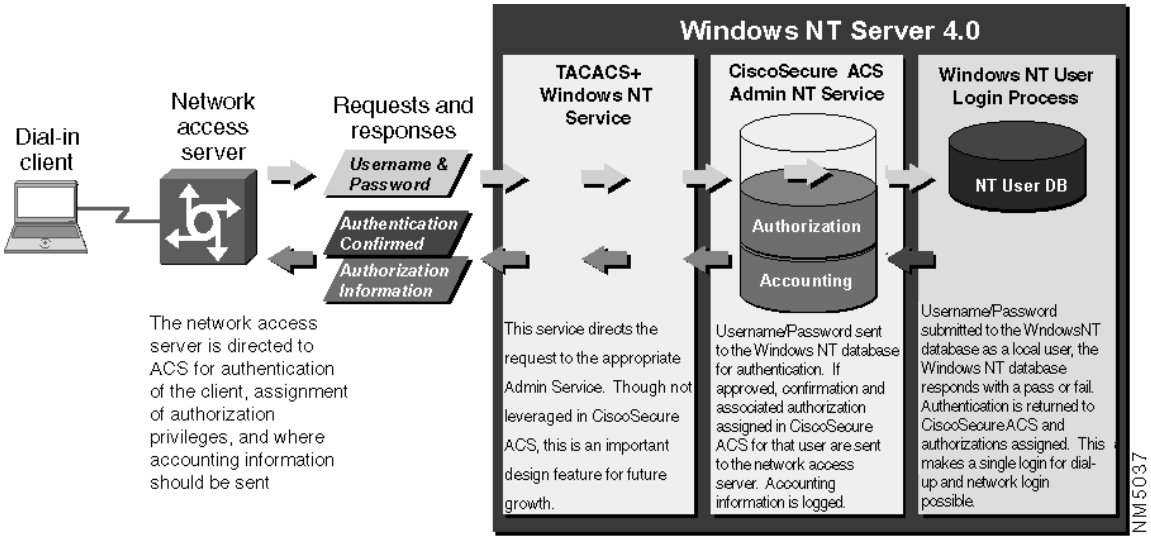
Cisco Secure ACS forwards user authentication requests to a Windows NT/2000 database in one of two scenarios. The first scenario is when the user's account in the CiscoSecure user database lists a Windows NT/2000 database configuration as the authentication method. The second is when the user is unknown to the CiscoSecure user database and the Unknown User Policy dictates that a Windows NT/2000 database is the next external user database to try.

In either case, Cisco Secure ACS forwards the username and password to the Windows NT/2000 database. The Windows NT/2000 database either passes or fails the authentication request from Cisco Secure ACS. Upon receiving the response from the Windows NT/2000 database, Cisco Secure ACS instructs the requesting AAA client to grant or deny the user access, depending upon the response from the Windows NT/2000 database.

Cisco Secure ACS grants authorization based on the Cisco Secure ACS group to which the user is assigned. While the group to which a user is assigned can be determined by information from the Windows NT/2000 database, it is Cisco Secure ACS that grants authorization privileges. See Figure 11-2 on page 11-8.

Downloaded from www.Manualslib.com manuals search engine

Figure 11-2 Using the Windows NT/2000 User Database for Authentication


Windows NT Server 4.0
TACACS+ Windows NT Service
CiscoSecure ACS Admin NT Service
Windows NT User Login Process
Dial-in client
Network access server
Requests and responses
Username & Password
Authentication Confirmed
Authorization Information
NT User DB
Authorization
Accounting
The network access server is directed to ACS for authentication of the client, assignment of authorization privileges, and where accounting information should be sent
This service directs the request to the appropriate Admin Service. Though not leveraged in CiscoSecure ACS, this is an important design feature for future growth.
Username/Password sent to the Windows NT database for authentication. If approved, confirmation and associated authorization assigned in CiscoSecure ACS for that user are sent to the network access server. Accounting information is logged.
Username/Password submitted to the WndowsNT database as a local user, the Windows NT database responds with a pass or fail. Authentication is returned to CiscoSecure ACS and authorizations assigned. This makes a single login for dial-up and network login possible.
NM5037

To further control access by a user from within the Windows NT User Manager or the Windows 2000 Active Directory Users and Computers, you can configure Cisco Secure ACS to also check the setting for granting dialin permission to user. This setting is labeled “Grant dialin permission to user” in Windows NT and “Allow access” in the Remote Access Permission area in Windows 2000. If this feature is disabled for the user, access is not permitted, even if the username and password are typed correctly.

For the most secure authentication with Windows NT/2000 user databases, use MS-CHAP.

Trust Relationships

Cisco Secure ACS can take advantage of trust relationships that have been established between Windows NT/2000 servers. If the domain that contains the Cisco Secure ACS server trusts another domain, Cisco Secure ACS can authenticate users whose accounts reside in the other domain. Cisco Secure ACS can also reference the Grant dialin permission to user setting across trusted domains.

If your domains are Windows 2000 domains, Cisco Secure ACS can take advantage of indirect trusts for Windows authentication. Consider the example of Windows 2000 domains A, B, and C, where Cisco Secure ACS resides on a

Downloaded from www.Manualslib.com manuals search engine

Windows 2000 server in domain A. Domain A trusts domain B, but no trust relationship is established between domain A and domain C. If domain B trusts domain C, the Cisco Secure ACS server in domain A can authenticate users whose accounts reside in domain C, making use of the indirect trust of domain C.

For more information on trust relationships, refer to your Microsoft Windows NT/2000 documentation.

Windows Dial-up Networking Clients

The dial-up networking clients for Windows NT/2000 and Windows 95/98/Millennium Edition (ME) allow users to connect to your network remotely, but the fields provided differ.

About the Windows NT/2000 Dial-up Networking Client

If you use the Windows NT/2000 Dial-Up Networking client to dial in to the AAA client, three fields appear:

- **username—**Type your username.
- **password—**Type your password.
- **domain—**Type your valid domain name.

Note For more information about the implications of completing or leaving the domain field blank, see the "Windows NT/2000 Authentication" section on page 11-10.

Downloaded from www.Manualslib.com manuals search engine

About the Windows 95/98/Millennium Edition Dial-up Networking Client

If you use the Windows 95/98/ME Dial-Up Networking client to dial in to the AAA client, two fields appear:

- **username—**Type your username.

Note You also have the option of prefixing your username with the name of the domain you want to log in to. For more information about the implications of prefixing or not prefixing the domain name before the username, see the "Windows NT/2000 Authentication" section on page 11-10.

- **password—**Type your password.

Windows NT/2000 Authentication

While the Windows NT/2000 and Windows 95/98/ME provide different methods of specifying a domain name, the effect of providing or not providing the domain name while logging in is the same.

The most reliable method of authenticating users against a specific domain is to require users to submit the domains they should be authenticated against along with their usernames. With the Windows NT/2000 dial-up client, this is accomplished by typing the domain in the domain field (or selecting it from the drop-down list). With the Windows 95/98/ME dial-up client, this is accomplished by submitting the username in the fully qualified format. Users submitting a fully qualified username must enter the domain name before their username in the following format:

```
DOMAIN_NAME\USER_NAME
```

For example, user Mary Smith (msmith) in Domain10 would enter the following:

```
Domain10\msmith
```

Another reason to provide the username in the format shown above is if a user is included in more than one domain. In this case, the privileges assigned upon authentication will be those associated with the account in the first domain with a

Downloaded from www.Manualslib.com manuals search engine

matching username and password. This also illustrates the importance of removing usernames from a domain when the privileges associated with the user are no longer required.

Tip For Windows 95/98/ME and Windows NT/2000, entering the domain name can speed up authentication, because Cisco Secure ACS can go directly to the domain rather than searching through the local domain and all trusted domains until it finds the username.

Note Cisco Secure ACS does not support the *user@domain* (UPN) format of qualified usernames when authenticating users with Windows user databases.

If you do not specify a domain name when typing the username, Cisco Secure ACS submits the username to the Windows NT/2000 operating system on the Cisco Secure ACS server. If the Windows NT/2000 server does not find the username in its local database, it then checks all trusted domains. If the password of the first occurrence of the username in the trusted domains does not match the password submitted by Cisco Secure ACS, authentication fails. If the Domain List in the Windows NT/2000 User Database Configuration of the External User Databases section has been configured with a list of trusted domains, Cisco Secure ACS submits the username and password to each domain in the list in a fully qualified format until it successfully authenticates the user. If Cisco Secure ACS has tried each domain listed in the Domain List or if no trusted domains have been configured in the Domain List, Cisco Secure ACS stops attempting to authenticate the user and does not grant that user access.

Note If your Domain List contains domains and your Windows SAM or Active Directory user databases are configured to lock out users after a number of failed attempts, users can be inadvertently locked out because Cisco Secure ACS tries each domain in the Domain List explicitly, resulting in failed attempts for identical usernames that reside in different domains.

Downloaded from www.Manualslib.com manuals search engine

User-Changeable Passwords with Windows NT/2000 User Databases

For network users who are authenticated by a Windows NT/2000 user database, Cisco Secure ACS supports the user-changeable passwords upon password expiration. You can enable this feature in the MS-CHAP Settings on the Windows NT/2000 User Database Configuration page in the External User Databases section. Using this feature in your network requires the following:

- Users must be present in the Windows NT/2000 user database
- User accounts in Cisco Secure ACS must specify the Windows NT/2000 user database for authentication
- End-user clients must be MS-CHAP compatible, such as the Windows dial-up networking client
- The network devices the end-user clients connect to must use RADIUS for authentication requests sent to Cisco Secure ACS

When the conditions above are met and this feature is enabled, users receive a dialog box prompting them to change their passwords upon their first successful authentication after their passwords have expired. The dialog box is the same as presented to users by Windows when a user with an expired password accesses a network via a remote access server.

Preparing Users for Authenticating with Windows NT/2000

Before using the Windows NT/2000 user database for authentication, follow these steps:

Step 1 Make sure the username exists in the Windows NT/2000 user database.

Step 2 In the Windows NT User Manager or in Windows 2000 Active Directory Users and Computers, clear the following User Properties check boxes:

- **User must change password at next logon**
- **Account disabled**

Downloaded from www.Manualslib.com manuals search engine

Step 3 If you want to control dial-in access from within Windows NT, click **Dial-in** and select **Grant dialin permission to user**. In Windows 2000, access the User Properties dialog box, select the **Dial-In** tab, and in the Remote Access area, click **Allow access**. You must also configure the option to reference this feature under Database Group Mappings in the External User Databases section of Cisco Secure ACS.

Configuring a Windows NT/2000 External User Database

To configure Cisco Secure ACS to authenticate users against the Windows NT/2000 user database in your network's trusted domains, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

Result: Cisco Secure ACS displays a list of all possible external user database types.

Step 3 Click **Windows NT/2000**.

Result: If no Windows NT/2000 database configuration exists, the Database Configuration Creation table appears. Otherwise, the External User Database Configuration page appears.

Step 4 If you are creating a new configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for Windows NT/2000 authentication in the box provided, or accept the default name in the box.

c. Click **Submit**.

Result: Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

Step 5 Click **Configure**.

Result: The Windows NT/2000 User Database Configuration page appears.

Downloaded from www.Manualslib.com manuals search engine

Step 6 To restrict network access to users who have Windows dial-in permission, select the **Grant dialin permission to user** check box.

Note Windows dialin permission is enabled in the Dialin section of user properties in Windows NT and on the Dial-in tab of the user properties in Windows 2000.

Step 7 To authenticate explicitly using each trusted Windows domain for usernames that are not domain-qualified, select the domains you want Cisco Secure ACS to use to authenticate unqualified usernames in the Available Domains list and move them to the Domain List list by clicking —>.

Step 8 In the MS-CHAP table, follow these steps:

a. To support for authentication, select the check boxes for the applicable MS-CHAP versions.

b. To enable password changes, select the check boxes for the applicable MS-CHAP versions.

Step 9 Click **Submit**.

Result: Cisco Secure ACS saves the Windows NT/2000 user database configuration you created. You can now add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see the "Unknown User Processing" section on page 12-1. For more information about configuring user accounts to authenticate using this database, see the "Setting Up and Managing User Accounts" section on page 7-1.

Generic LDAP

Cisco Secure ACS supports PAP and EAP-TLS authentication via generic Lightweight Directory Access Protocol (LDAP) databases, such as Netscape Directory Services. Configuring Cisco Secure ACS to authenticate against an LDAP database does not affect the configuration of the LDAP database. To manage your LDAP database, see your LDAP database documentation.

Downloaded from www.Manualslib.com manuals search engine

This section contains the following topics:

- Cisco Secure ACS Authentication Process with a Generic LDAP User Database, page 11-15
- Multiple LDAP Instances, page 11-16
- LDAP Organizational Units and Groups, page 11-17
- Directed Authentications, page 11-17
- LDAP Failover, page 11-17
- Configuring a Generic LDAP External User Database, page 11-19

Cisco Secure ACS Authentication Process with a Generic LDAP User Database

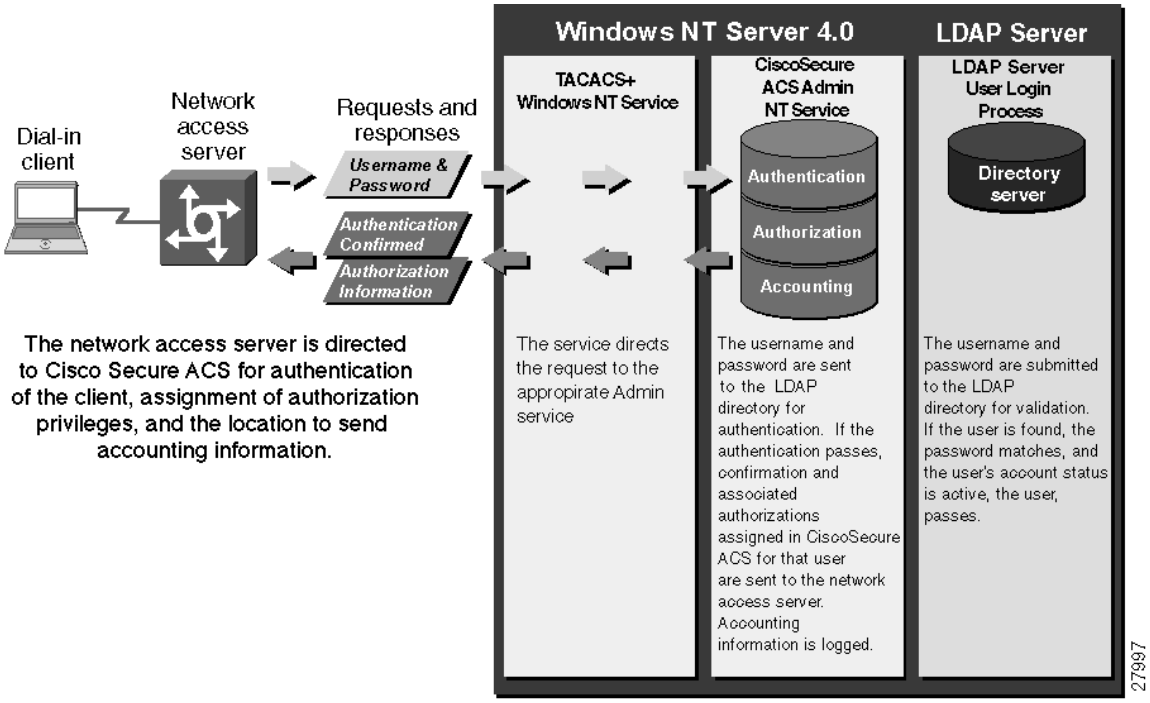
Cisco Secure ACS forwards user authentication requests to an LDAP database in one of two scenarios. The first scenario is when the user's account in the CiscoSecure user database lists an LDAP configuration as the authentication method. The second is when the user is unknown to the CiscoSecure user database and the Unknown User Policy dictates that an LDAP database is the next external user database to try.

In either case, Cisco Secure ACS forwards the username and password to the LDAP database. The LDAP database either passes or fails the authentication request from Cisco Secure ACS. Upon receiving the response from the LDAP database, Cisco Secure ACS instructs the requesting AAA client to grant or deny the user access, depending upon the response from the LDAP server.

Cisco Secure ACS grants authorization based on the Cisco Secure ACS group to which the user is assigned. While the group to which a user is assigned can be determined by information from the LDAP server, it is Cisco Secure ACS that grants authorization privileges. See Figure 11-3 on page 11-16.

Downloaded from www.Manualslib.com manuals search engine

Figure 11-3 Using an LDAP Server for Authentication


Windows NT Server 4.0
LDAP Server
Dial-in client
Network access server
Requests and responses
Username & Password
Authentication Confirmed
Authorization Information
TACACS+ Windows NT Service
CiscoSecure ACS Admin NT Service
LDAP Server User Login Process
Authentication
Authorization
Accounting
Directory server
The network access server is directed to Cisco Secure ACS for authentication of the client, assignment of authorization privileges, and the location to send accounting information.
The service directs the request to the appropirate Admin service
The username and password are sent to the LDAP directory for authentication. If the authentication passes, confirmation and associated authorizations assigned in CiscoSecure ACS for that user are sent to the network access server. Accounting information is logged.
The username and password are submitted to the LDAP directory for validation. If the user is found, the password matches, and the user's account status is active, the user, passes.
27997

Multiple LDAP Instances

You can create several LDAP configurations in Cisco Secure ACS. For each LDAP configuration, you can add or leave it out of the Unknown User Policy. Also for each LDAP configuration, you can establish unique group mapping.

Cisco Secure ACS does not require that each LDAP instance corresponds to a unique LDAP database. You can have more than one LDAP configuration set to access the same database. This is useful when your LDAP database contains more than one subtree for users or groups. Because each LDAP configuration supports only one subtree directory for users and one subtree directory for groups, you must configure separate LDAP instances for each user directory subtree and group directory subtree combination for which Cisco Secure ACS should submit authentication requests.

Downloaded from www.Manualslib.com manuals search engine

LDAP Organizational Units and Groups

LDAP groups do not need to have the same name as their corresponding Cisco Secure ACS groups. The LDAP group can be mapped to a Cisco Secure ACS group with any name you want to assign. For more information about how your LDAP database handles group membership, see your LDAP database documentation. For more information on LDAP group mappings and Cisco Secure ACS, see the "Database Group Mappings" section on page 12-10.

Directed Authentications

You can configure Cisco Secure ACS to filter user authentications that it submits to LDAP databases. Filtering is based on a string of characters either at the beginning or end of the username submitted for authentication. This enables you to have greater control over which LDAP instance Cisco Secure ACS submits user authentication requests. For example, you could configure a different LDAP instance per domain in your network and direct the authentications for each as applicable.

Depending upon how an LDAP database is configured, the different LDAP instances in Cisco Secure ACS can authenticate users using the same LDAP database but with different contexts. Using directed authentications in conjunction with this flexibility allows you to specify which user and group directory subtrees the LDAP database uses to authenticate users of a given domain.

LDAP Failover

Cisco Secure ACS supports failover between a primary server and secondary LDAP server. In the context of LDAP authentication with Cisco Secure ACS, failover applies when an authentication request fails because Cisco Secure ACS could not connect to an LDAP server, such as when the server is down or is otherwise unreachable by the Cisco Secure ACS server. To use this feature, you must define the primary and secondary LDAP servers on the LDAP Database Configuration page. Also, you must select the On Timeout Use Secondary check box. For more information about configuring an LDAP external user database, see the "Configuring a Generic LDAP External User Database" section on page 11-19.

Downloaded from www.Manualslib.com manuals search engine

If the On Timeout Use Secondary check box is selected, and if the first LDAP server that Cisco Secure ACS attempts to contact cannot be reached, Cisco Secure ACS always attempts to contact the other LDAP server. The first server Cisco Secure ACS attempts to contact may not always be the primary LDAP server. Instead, the first LDAP server that Cisco Secure ACS attempts to contact depends on the previous LDAP authentication attempt and on the value specified in the Failback Retry Delay box.

Successful Previous Authentication with the Primary LDAP Server

If, on the previous LDAP authentication attempt, Cisco Secure ACS successfully connected to the primary LDAP server, Cisco Secure ACS attempts to connect to the primary LDAP server. If Cisco Secure ACS cannot connect to the primary LDAP server, Cisco Secure ACS attempts to connect to the secondary LDAP server.

If Cisco Secure ACS cannot connect with either LDAP server, Cisco Secure ACS stops attempting LDAP authentication for the user. If the user is an unknown user, Cisco Secure ACS tries the next external user database listed in the Unknown User Policy list. For more information about the Unknown User Policy list, see the "Unknown User Processing" section on page 12-1.

Unsuccessful Previous Authentication with the Primary LDAP Server

If, on the previous LDAP authentication attempt, Cisco Secure ACS could not connect to the primary LDAP server, whether Cisco Secure ACS first attempts to connect to the primary server or secondary LDAP server for the current authentication attempt depends on the value in the Failback Retry Delay box. If the Failback Retry Delay box is set to 0 (zero), Cisco Secure ACS always attempts to connect to the primary LDAP server first. And if Cisco Secure ACS cannot connect to the primary LDAP server, Cisco Secure ACS then attempts to connect to the secondary LDAP server.

If the Failback Retry Delay box is set to a number other than zero, Cisco Secure ACS determines how many minutes have passed since the last authentication attempt using the primary LDAP server occurred. If more minutes have passed than the value specified in the Failback Retry Delay box, Cisco Secure ACS attempts to connect to the primary LDAP server first. And if Cisco Secure ACS cannot connect to the primary LDAP server, Cisco Secure ACS then attempts to connect to the secondary LDAP server.

Downloaded from www.Manualslib.com manuals search engine

If fewer minutes have passed than the value specified in the Failback Retry Delay box, Cisco Secure ACS attempts to connect to the secondary LDAP server first. And if Cisco Secure ACS cannot connect to the secondary LDAP server, Cisco Secure ACS then attempts to connect to the primary LDAP server.

If Cisco Secure ACS cannot connect to either LDAP server, Cisco Secure ACS stops attempting LDAP authentication for the user. If the user is an unknown user, Cisco Secure ACS tries the next external user database listed in the Unknown User Policy list. For more information about the Unknown User Policy list, see the "Unknown User Processing" section on page 12-1.

Configuring a Generic LDAP External User Database

Creating a generic LDAP configuration provides Cisco Secure ACS information that enables it to pass authentication requests to an LDAP database. This information reflects the way you have implemented your LDAP database and does not dictate how your LDAP database is configured or functions. For information about your LDAP database, refer to your LDAP documentation.

To configure Cisco Secure ACS to use the LDAP User Database, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

Result: Cisco Secure ACS displays a list of all possible external user database types.

Step 3 Click **Generic LDAP**.

Note The user authenticates against only one LDAP database.

Result: If no LDAP database configuration exists, only the Database Configuration Creation table appears. Otherwise, in addition to the Database Configuration Creation table, the External User Database Configuration table appears.

Downloaded from www.Manualslib.com manuals search engine

Step 4 If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for generic LDAP in the box provided.

c. Click **Submit**.

Result: Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

Step 5 Under External User Database Configuration, select the name of the LDAP database you need to configure.

Note If only one LDAP configuration exists, the name of that configuration appears instead of the list. Proceed to the next step.

Step 6 Click **Configure**.

Caution If you click Delete, the configuration of the selected LDAP database is deleted.

Step 7 To enable Cisco Secure ACS to process LDAP authentications without domain filtering, from the Filter Domains list, select **No**.

Step 8 To enable Cisco Secure ACS to direct LDAP authentications by filtering on the beginning of a username, follow these steps:

a. From the Filter Domains list, select **Prefix**.

b. In the Domain Markup box, type the string of characters that a username must begin with in order for Cisco Secure ACS to use this LDAP configuration for authentication.

For example, if users to be authenticated by this LDAP configuration submit a username that begins with “ofc1-”, such as ofc1-stanley or ofc1-mwiliams, type **ofc1-** in the Domain Markup box.

c. To remove from the beginning of the username the characters defined in the Domain Markup box before submitting it to the LDAP database, select the **Strip Markup** check box.

d. To pass the username to the LDAP database *without* removing the characters defined in Domain Markup, clear the **Strip Markup** check box.

Downloaded from www.Manualslib.com manuals search engine

Step 9 To enable Cisco Secure ACS to direct LDAP authentications by filtering on the end of a username, follow these steps:

a. From the Filter Domains list, select **Suffix**.

b. In the Domain Markup box, type the string of characters that a username must end with in order for Cisco Secure ACS to use this LDAP configuration for authentication.

For example, if users to be authenticated by this LDAP configuration submit a username that ends with "@mydomain.com", such as stanley@mydomain.com or mwiliams@mydomain.com, in the Domain Markup box, type **@mydomain.com**.

c. To remove from the end of the username the characters defined in the Domain Markup box before submitting it to the LDAP database, select the **Strip Markup** check box.

d. To pass the username to the LDAP database *without* removing the characters defined in Domain Markup, clear the **Strip Markup** check box.

Step 10 In the User Directory Subtree box, type the following:

o=*subtree*

where *subtree* is the tree in which all of your users are located. This is configured when you set up your LDAP database. For more information, refer to your LDAP database documentation.

Note Your users could be located under an organizational unit rather than an organization. If this is the case, type **ou=** *subtree* in the User Directory Subtree.

Step 11 In the Group Directory Subtree box, type the following:

o=*subtree*

where *subtree* is the tree in which all of your groups are located. This can be the same location as the user subtree, entered in the User Directory Subtree box. This is configured when you set up your LDAP database. For more information, refer to your LDAP database documentation.

Downloaded from www.Manualslib.com manuals search engine

Note Your groups could be located under an organizational unit rather than an organization. If this is the case, in the Group Directory Subtree, type ou=*subtree*.

Step 12 In the User Object Type box, type the name of the attribute in the user record that contains the user name. You can obtain this attribute name from your Directory Server. For more information, refer to your LDAP database documentation.

Note The default values in the UserObjectType and following fields reflect the default configuration of the Netscape Directory Server. Confirm all values for these fields with your LDAP server's configuration and documentation.

Step 13 In the User Object Class box, type the value of the LDAP "objectType" attribute that identifies the record as a user. Often, user records have several values for the objectType attribute, some of which are unique to the user, some of which are shared with other object types. Select a value that is not shared.

Step 14 In the GroupObjectType box, type the name of the attribute in the group record that contains the group name.

Step 15 In the GroupObjectClass box, type a value of the LDAP "objectType" attribute in the group record that identifies the record as a group.

Step 16 In the GroupAttributeName box, type the name of the attribute of the group record that contains the list of user records who are a member of that group.

Step 17 In the Server Timeout box, type the number of seconds Cisco Secure ACS waits for a response from an LDAP server before determining that the connection with that server has failed.

Step 18 To enable failover of LDAP authentication attempts, select the **On Timeout Use Secondary** check box. For more information about the LDAP failover feature, see the "LDAP Failover" section on page 11-17.

Step 19 In the Failback Retry Delay box, type the number of minutes after the primary LDAP server fails to authenticate a user that Cisco Secure ACS resumes sending authentication requests to the primary LDAP server first.

Downloaded from www.Manualslib.com manuals search engine

Note To specify that Cisco Secure ACS should always use the primary LDAP server first, type `0` (zero) in the Failback Retry Delay box.

Step 20 For the Primary LDAP Server and Secondary LDAP Server tables, follow these steps:

Note If you did not select the On Timeout Use Secondary check box, you do not need to complete the options in the Secondary LDAP Server table.

a. In the Hostname box, type the name or IP address of the machine that is running the LDAP software. If you are using DNS on your network, you can type the hostname instead of the IP address.

b. In the Port box, type the TCP/IP port number on which the LDAP server is listening. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information by viewing those properties on the LDAP server. If you want to use secure authentication, port number 636 is usually used.

c. To specify that Cisco Secure ACS should use LDAP version 3 to communicate with your LDAP database, select the **LDAP Version** check box. If the LDAP Version check box is not selected, Cisco Secure ACS uses LDAP version 2.

d. The username and password credentials are normally passed over the network to the LDAP directory in clear text. To enhance security, select the **Use secure authentication** check box.

e. In the Certificate Database Path box, type the path to the `cert7.db` file, which contains the certificates for the server to be queried and the trusted CA.

f. The Admin DN box requires the fully qualified (DN) of the administrator; that is, the LDAP account which, if bound to, permits searches for all required users under the User Directory Subtree.

Downloaded from www.Manualslib.com manuals search engine

In the Admin DN box, type the following information from your LDAP server:

`uid=`*user id*`,[ou=`*organizational unit*`,][ou=`*next organizational unit*`]o=`*organization*

where *user id* is the username

organizational unit is the last level of the tree

next organizational unit is the next level up the tree.

For example:

```
uid=joesmith,ou=members,ou=administrators,o=cisco
```

Tip If you are using Netscape DS, you can copy this information from the Netscape Console.

For more information, refer to your LDAP database documentation.

g. In the Password box, type the password for the administrator account specified in the Admin DN box. Password case sensitivity is determined by the server.

Step 21 Click **Submit**.

Result: Cisco Secure ACS saves the generic LDAP configuration you created. You can now add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see the "Unknown User Processing" section on page 12-1. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "Setting Up and Managing User Accounts."

Novell NDS Database

Cisco Secure ACS supports PAP authentication with Novell NetWare Directory Services (NDS) servers. To use NDS authentication, you must have a Novell NDS database. Configuring Cisco Secure ACS to authenticate against an NDS database does not affect the configuration of the NDS database. To manage your NDS database, refer to your NDS database documentation.

Downloaded from www.Manualslib.com manuals search engine

Some versions of Novell NDS provide standard LDAP implementations. If your Novell NDS supports standard LDAP and you have implemented standard LDAP, you should configure a Cisco Secure ACS generic LDAP external user database to authenticate users defined in your Novell NDS. For more information about generic LDAP external user databases, see the "Generic LDAP" section on page 11-14.

To authenticate users with a Novell NDS database, Cisco Secure ACS depends upon Novell Requestor. Novell Requestor must be installed on the same Windows NT/2000 server as Cisco Secure ACS. You can download the Requestor software from the Novell web site. For more information, refer to your Novell and Microsoft documentation.

For users to authenticate against a Novell NDS database, Cisco Secure ACS must be correctly configured to recognize the Novell NDS structure. Cisco Secure ACS supports up to twenty trees. Each tree has several containers, and each container can have several contexts. NDS trees can be thought of as similar to Windows NT/2000 domains. For a user to authenticate against a Novell NDS context, a user object must exist, and the password must be able to log the name into the tree.

This section contains the following topics:

- User Contexts, page 11-25
- Novell NDS External User Database Options, page 11-27
- Configuring a Novell NDS External User Database, page 11-28

User Contexts

You must supply one or more contexts when you configure Cisco Secure ACS to authenticate with an NDS database; however, users can supply an additional portion of the full context that defines their fully-qualified usernames. In other words, if none of the contexts in the list of contexts contains a username submitted for authentication, the username must specify exactly how they are subordinate to the contexts in the list of contexts. The user specifies the manner in which a username is subordinate to a context by providing the additional context information needed to uniquely identify the user in the NDS database.

Downloaded from www.Manualslib.com manuals search engine

Consider the following example tree:

```
[Root] whose treename=ABC
 OU=ABC-Company
  OU=sales
     CN=Agamemnon
  OU=marketing
    CN=Odysseus
    OU=marketing-research
       CN=Penelope
    OU=marketing-product
       CN=Telemachus
```

If the context list configured in Cisco Secure ACS were:

```
ABC-Company,sales.ABC-Company
```

then Agamemnon would successfully authenticate if he submitted "Agamemnon.sales" as his username. If he submitted only "Agamemnon", authentication would fail.

Table 11-1 lists the users given in the example tree and the username with context that would allow each user to authenticate successfully.

Table 11-1 Example Usernames with Contexts

User	Valid Username With Context
Agamemnon	Agamemnon
Odysseus	Odysseus.marketing
Penelope	Penelope.marketing-research.marketing
Telemachus	Telemachus.marketing-product.marketing

Downloaded from www.Manualslib.com manuals search engine

Novell NDS External User Database Options

You create and maintain configurations for Novell NDS database authentication on the NDS Authentication Support page in Cisco Secure ACS. This page enables you to add a configuration for a Novell NDS tree, change existing tree configurations, and delete existing tree configurations in a single submission to the Cisco Secure ACS web server. Cisco Secure ACS displays information for each tree configured, plus a blank section for creating a tree. The configuration items presented for each tree are as follows:

- **Add New Tree—**Appears only on the blank form for new trees. Selecting this check box confirms that you want to add a new tree.
- **Delete Tree—**Appears only on existing tree configurations. Selecting this check box indicates that you want to delete the tree configuration when you click Submit.
- **Test Login—**Selecting this check box causes Cisco Secure ACS to test the the tree's administrative login to the Novell server when you click Submit.
- **Tree Name—**Appears only on the blank form for new trees. The name of the Novell NDS tree against which Cisco Secure ACS should authenticate users.
- **Administrator Username—**The fully qualified, typeless username for the administrator of the Novell server. For example:

  ```
  admin.Chicago.Corporation
  ```

- **Administrator Password—**The password for the administrator of the Novell server.
- **Context List—**The full context list with each context specified in canonical, typeless form; that is, remove the `o=` and `ou=` and separate each part of the context using a period (.). You can enter more than one context list. If you do, separate them with a comma. For example, if your Organization is Corporation, your Organization Name is Chicago, and you want to enter two Context names, Marketing and Engineering, you would type:

  ```
  Engineering.Chicago.Corporation, Marketing.Chicago.Corporation
  ```

  You do not need to add users in the Context List box.

Note Users can provide a portion of their context when they login. For more information, see the "User Contexts" section on page 11-25.

Downloaded from www.Manualslib.com manuals search engine

Configuring a Novell NDS External User Database

You can allow users to enter their own context as part of the login process.

Creating an Novell NDS database configuration is a process that provides Cisco Secure ACS information that enables it to pass authentication requests to an NDS database. This information reflects the way you have implemented your NDS database and does not dictate how your NDS database is configured or functions. For information about your NDS database, refer to your Novell NDS documentation.

Before You Begin

The Novell Requestor Software for Novell NDS must be installed on the same Windows NT server as Cisco Secure ACS. If the Novell Requestor Software for Novell NDS is not on the same Windows NT server as Cisco Secure ACS, you cannot complete this procedure.

To configure Novell NDS authentication, follow these steps:

Step 1 See your Novell NetWare administrator to get the names and other information on the Tree, Container, and Context.

Step 2 In the navigation bar, click **External User Databases**.

Step 3 Click **Database Configuration**.

Result: Cisco Secure ACS displays a list of all possible external user database types.

Step 4 Click **Novell NDS**.

Result: If no Novell NDS database has yet been configured, the Database Configuration Creation page appears. Otherwise, the External User Database Configuration page appears.

Step 5 If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for Novell NDS Authentication in the box provided.

c. Click **Submit**.

Result: Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

Downloaded from www.Manualslib.com manuals search engine

Step 6 Click **Configure**.

Caution If you click Delete, the Cisco Secure ACS configuration for your Novell NDS database is deleted.

Result: The NDS Authentication Support page appears. The NDS Authentication Support page enables you to add a configuration for an Novell NDS tree, change existing tree configurations, and delete existing tree configurations.

For more information about the content of the NDS Authentication Support page, see the "Novell NDS External User Database Options" section on page 11-27.

Step 7 To add a new tree configuration, complete the fields in the blank form at the bottom of the NDS Authentication Support page.

Note You must select the Add Tree check box to confirm that you want to create a tree configuration.

Step 8 To change an existing tree configuration, edit the values you need to change.

Note The name of a tree is not changeable. If you need to change a tree name, click **Delete Tree?** on the misnamed tree's section and click **Submit**. Then, add a new tree with the same configuration data as the deleted, misnamed tree, making sure the tree name is correct before clicking Submit.

Step 9 To delete an existing tree configuration, select the **Delete Tree** check box.

Step 10 Click **Submit**.

Result: Cisco Secure ACS saves the NDS configuration you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see the "Unknown User Processing" section on page 12-1. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "Setting Up and Managing User Accounts."

Downloaded from www.Manualslib.com manuals search engine

ODBC Database

Cisco Secure ACS supports PAP, CHAP, MS-CHAP, and ARAP authentication using a relational database via the ODBC authenticator feature. As with Windows NT/2000 database support, Cisco Secure ACS's ODBC-compliant relational database support enables you to make use of existing user records held in an external ODBC-compliant relational database. Configuring Cisco Secure ACS to authenticate against an ODBC-compliant relational database does not affect the configuration of the relational database. To manage your relational database, refer to your relational database documentation.

The Windows ODBC feature enables you to create a data source name (DSN), which specifies the database and other important parameters necessary for communicating with the database. Among the parameters you provide are the username and password required for the ODBC driver to gain access to your ODBC-compliant relational database.

This section contains the following topics:

- Cisco Secure ACS Authentication Process with an ODBC External User Database, page 11-31
- Preparing to Authenticate Users with an ODBC-Compliant Relational Database, page 11-32
- Implementation of Stored Procedures for ODBC Authentication, page 11-33
- Microsoft SQL Server and Case-Sensitive Passwords, page 11-34
- Sample Routine for Generating a PAP Authentication SQL Procedure, page 11-35
- Sample Routine for Generating an SQL CHAP Authentication Procedure, page 11-36
- PAP Authentication Procedure Input, page 11-36
- PAP Procedure Output, page 11-37
- CHAP/MS-CHAP/ARAP Authentication Procedure Input, page 11-38
- CHAP/MS-CHAP/ARAP Procedure Output, page 11-38
- Result Codes, page 11-39

Downloaded from www.Manualslib.com manuals search engine

- Configuring a System Data Source Name for an ODBC External User Database, page 11-40
- Configuring an ODBC External User Database, page 11-41

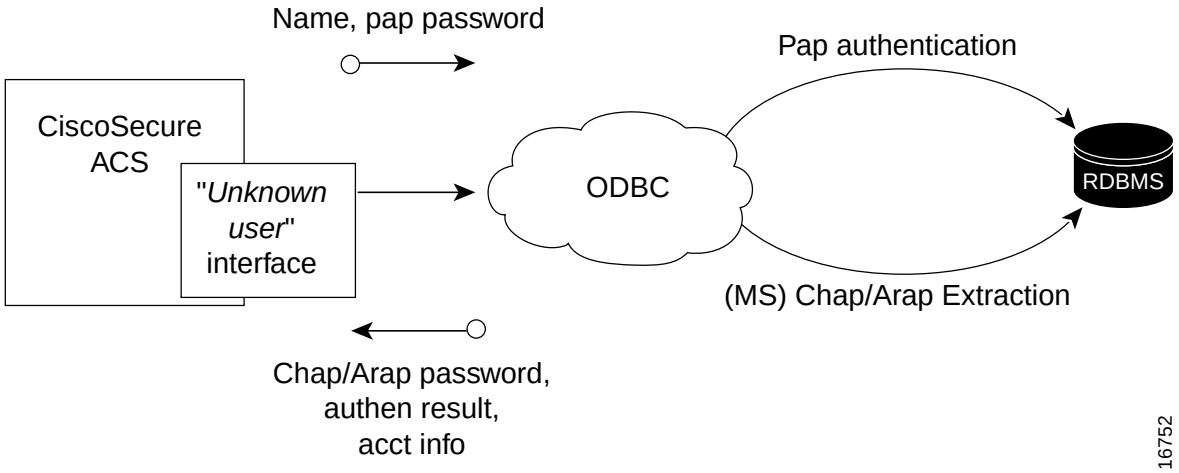
Cisco Secure ACS Authentication Process with an ODBC External User Database

Cisco Secure ACS forwards user authentication requests to an ODBC database in one of two scenarios. The first scenario is when the user's account in the CiscoSecure user database lists an ODBC database configuration as the authentication method. The second is when the user is unknown to the CiscoSecure user database and the Unknown User Policy dictates that an ODBC database is the next external user database to try.

In either case, Cisco Secure ACS forwards the username and password to the ODBC database via an ODBC connection. The ODBC database either passes or fails the authentication request from Cisco Secure ACS. The relational database must have a stored procedure that queries the appropriate tables and returns values to Cisco Secure ACS. If the returned values indicate that the username and password provided are valid, Cisco Secure ACS instructs the requesting AAA client to grant the user access; otherwise, Cisco Secure ACS denies the user access. See Figure 11-4. Upon receiving the response from the ODBC database, Cisco Secure ACS instructs the requesting AAA client to grant or deny the user access, depending upon the response from the ODBC database.

Downloaded from www.Manualslib.com manuals search engine

Figure 11-4 Using the ODBC Database for Authentication



Cisco Secure ACS grants authorization based on the Cisco Secure ACS group to which the user is assigned. While the group to which a user is assigned can be determined by information from the ODBC database using a process known as “group specification”, it is Cisco Secure ACS that grants authorization privileges.

Cisco Secure ACS passes the user information to the relational database via the ODBC connection. The relational database must have a stored procedure that queries the appropriate tables and returns values to Cisco Secure ACS. If the returned values indicate that the username and password provided are valid, Cisco Secure ACS grants the user access. Otherwise, Cisco Secure ACS denies the user access. See Figure 11-4 on page 11-32.

Preparing to Authenticate Users with an ODBC-Compliant Relational Database

Authenticating users with an ODBC-compliant relational database requires that you complete several significant steps external to Cisco Secure ACS before configuring Cisco Secure ACS with an ODBC external user database.

Downloaded from www.Manualslib.com manuals search engine

To prepare for authenticating with an ODBC-compliant relational database, follow these steps:

Step 1 Install the database software on its server. For more information, refer to the relational database documentation.

Step 2 Create the database to hold the usernames and passwords. The database name is irrelevant to Cisco Secure ACS, so you can name the database however you like.

Step 3 Create the table or tables that will hold the usernames and passwords for your users. The table names are irrelevant to Cisco Secure ACS, so you can name the tables and columns however you like.

Step 4 Write the stored procedures intended to return the required authentication information to Cisco Secure ACS. For more information about these stored procedures, see the "Implementation of Stored Procedures for ODBC Authentication" section on page 11-33.

Step 5 Set up a system DSN on the Cisco Secure ACS server. For steps, see the "Configuring a System Data Source Name for an ODBC External User Database" section on page 11-40.

Step 6 Configure Cisco Secure ACS to authenticate users with an ODBC database. For steps, see the "Configuring an ODBC External User Database" section on page 11-41.

Implementation of Stored Procedures for ODBC Authentication

When you configure Cisco Secure ACS to authenticate users against an ODBC-compliant relational database, you must create a stored procedure to perform the necessary query and return the values that Cisco Secure ACS expects. Cisco Secure ACS supports ODBC authentication for PAP or CHAP/MS-CHAP/ARAP protocols; however, the method of authentication differs for these two sets of protocols.

Authentication for PAP protocol occurs within the relational database; that is, if the stored procedure finds a record with both the username and the password matching the input, the user is considered authenticated.

Downloaded from www.Manualslib.com manuals search engine

Authentication for CHAP/MS-CHAP/ARAP occurs within Cisco Secure ACS. The stored procedure returns the fields for the record with a matching username, including the password. Cisco Secure ACS confirms or denies authentication based on the values returned from the procedure.

To support the two protocols, Cisco Secure ACS provides different input to, and expects different output from, the ODBC authentication request. This requires a separate stored procedure in the relational database to support each protocol.

The Cisco Secure ACS product CD provides "stub" routines for creating a procedure in either Microsoft SQL Server or an Oracle database. You can either modify a copy of these routines to create your stored procedure or write your own. Example routines for creating PAP and CHAP/MS-CHAP/ARAP authentication stored procedures in SQL Server are given in the "Sample Routine for Generating a PAP Authentication SQL Procedure" section on page 11-35 and the "Sample Routine for Generating an SQL CHAP Authentication Procedure" section on page 11-36.

The following sections provide reference information about Cisco Secure ACS data types versus SQL data types, PAP authentication procedure inputs and outputs, CHAP/MS-CHAP/ARAP authentication procedure inputs and outputs, and expected result codes. You can use this information while writing your authentication stored procedures in your relational database.

Type Definitions

The Cisco Secure ACS types and their matching SQL types are as follows:

- **Integer—**SQL_INTEGER
- **String—**SQL_CHAR or SQL_VARCHAR

Microsoft SQL Server and Case-Sensitive Passwords

If you want your passwords to be case sensitive and are using Microsoft SQL Server as your ODBC-compliant relational database, configure your SQL Server to accommodate this feature. If your users are authenticating using PPP via PAP or Telnet login, the password might not be case sensitive, depending on how the case-sensitivity option is set on the SQL Server. For example, an Oracle database

Downloaded from www.Manualslib.com manuals search engine

will default to case sensitive, whereas Microsoft SQL Server defaults to case insensitive. However, in the case of CHAP/ARAP, the password is case sensitive if the CHAP stored procedure is configured.

For example, with Telnet or PAP authentication, the passwords **cisco** or **CISCO** or **CiScO** will all work if the SQL Server is configured to be case insensitive.

For CHAP/ARAP, the passwords **cisco** or **CISCO** or **CiScO** are not the same, regardless of whether or not the SQL Server is configured for case-sensitive passwords.

Sample Routine for Generating a PAP Authentication SQL Procedure

The following example routine creates a procedure named CSNTAuthUserPap in Microsoft SQL Server, the default procedure used by Cisco Secure ACS for PAP authentication. Table and column names that could vary for your database schema are presented in variable text. The Cisco Secure ACS product CD includes a stub routine for creating a procedure in either SQL Server or Oracle. For more information about data type definitions, procedure parameters, and procedure results, see the "ODBC Database" section on page 11-30.

```
if exists (select * from sysobjects where id = object_id
(`dbo.CSNTAuthUserPap') and sysstat & 0xf = 4)
drop procedure dbo.CSNTAuthUserPap
GO

CREATE PROCEDURE CSNTAuthUserPap
@username varchar(64), @pass varchar(255)
AS
SET NOCOUNT ON
IF EXISTS( SELECT username
FROM users
WHERE username = @username
AND csntpassword = @pass )
SELECT 0,csntgroup,csntacctinfo,"No Error"
FROM users
WHERE username = @username
ELSE
SELECT 3,0,"odbc","ODBC Authen Error"

GO
GRANT EXECUTE ON dbo.CSNTAuthUserPap TO ciscosecure
GO
```


Downloaded from www.Manualslib.com manuals search engine

Sample Routine for Generating an SQL CHAP Authentication Procedure

The following example routine creates in Microsoft SQL Server a procedure named CSNTExtractUserClearTextPw, the default procedure used by Cisco Secure ACS for CHAP/MS-CHAP/ARAP authentication. Table and column names that could vary for your database's schema are presented in variable text. For more information about data type definitions, procedure parameters, and procedure results, see the "ODBC Database" section on page 11-30.

```
if exists (select * from sysobjects where id =
object_id(`dbo.CSNTExtractUserClearTextPw') and sysstat & 0xf = 4)
drop procedure dbo.CSNTExtractUserClearTextPw
GO

CREATE PROCEDURE CSNTExtractUserClearTextPw
@username varchar(64)
AS
SET NOCOUNT ON
IF EXISTS( SELECT username
FROM users
WHERE username = @username )
SELECT 0,csntgroup,csntacctinfo,"No Error",csntpassword
FROM users
WHERE username = @username
ELSE
SELECT 3,0,"odbc","ODBC Authen Error"
GO

GRANT EXECUTE ON dbo.CSNTExtractUserClearTextPw TO ciscosecure
GO
```

PAP Authentication Procedure Input

Table 11-2 details the input provided by Cisco Secure ACS to the stored procedure supporting PAP authentication. The stored procedure should accept the named input values as variables.

Downloaded from www.Manualslib.com manuals search engine

Table 11-2 PAP Stored Procedure Input

Field	Type	Explanation
CSNTusername	String	0-64 characters
CSNTpassword	String	0-255 characters

The input names are for guidance only. Procedure variables created from them can have different names; however, they must be defined in the procedure in the order shown—the username must precede the password variable.

PAP Procedure Output

The stored procedure must return a single row containing the non-null fields. Table 11-3 lists the procedure results Cisco Secure ACS expects as output from stored procedure.

Table 11-3 PAP Stored Procedure Results

Field	Type	Explanation
CSNTresult	Integer	See Table 11-6 on page 11-39.
CSNTgroup	Integer	The Cisco Secure ACS group number for authorization. 0xFFFFFFFF is used to assign the default value. Values other than 0-499 are converted to the default. **Note** The group specified in the CSNTgroup field overrides group mapping configured for the ODBC external user database.
CSNTacctInfo	String	0-16 characters. A third-party defined string is added to subsequent account log file entries.
CSNTerror String	String	0-255 characters. A third-party defined string is written to the CSAuth service log file if an error occurs.

Downloaded from www.Manualslib.com manuals search engine

The CSNTGroup and CSNTacctInfo fields are processed only after a successful authentication. The CSNTerrorString file is logged only after a failure (if the result is greater than or equal to 4).

The procedure must return the result fields in the order listed above.

CHAP/MS-CHAP/ARAP Authentication Procedure Input

Cisco Secure ACS provides a single value for input to the stored procedure supporting CHAP/MS-CHAP/ARAP authentication. The stored procedure should accept the named input value as a variable.

Note Because Cisco Secure ACS performs authentication for CHAP/MS-CHAP/ARAP, the user's password is not an input. See Table 11-4.

Table 11-4 CHAP Stored Procedure Input

Field	Type	Explanation
CSNTusername	String	0-64 characters

The input name is for guidance only. A procedure variable created from it can have a different name.

CHAP/MS-CHAP/ARAP Procedure Output

The stored procedure must return a single row containing the non-null fields. Table 11-5 lists the procedure results Cisco Secure ACS expects as output from stored procedure.

Downloaded from www.Manualslib.com manuals search engine

Table 11-5 CHAP/MS-CHAP/ARAP Stored Procedure Results

Field	Type	Explanation
CSNTresult	Integer	See Table 11-6 on page 11-39 Result Codes.
CSNTgroup	Integer	The Cisco Secure ACS group number for authorization. 0xFFFFFFFF is used to assign the default value. Values other than 0-499 are converted to the default. **Note** The group specified in the CSNTgroup field overrides group mapping configured for the ODBC external user database.
CSNTacctInfo	String	0-16 characters. A third-party defined string is added to subsequent account log file entries.
CSNTerror-String	String	0-255 characters. A third-party defined string is written to the CSAuth service log file if an error occurs.
CSNTpass-word	String	0-255 characters. The password is authenticated by Cisco Secure ACS for CHAP authentication.

The CSNTGroup and CSNTacctInfo fields are processed only after a successful authentication. The CSNTerrorString file is logged only after a failure (if the result is greater than or equal to 4).

The procedure must return the result fields in the order listed above.

Result Codes

You can set the result codes listed in Table 11-6.

Table 11-6 Result Codes

Result Code	Meaning
0 (zero)	Authentication successful
1	Unknown username
2	Invalid password

Downloaded from www.Manualslib.com manuals search engine

Table 11-6 Result Codes (continued)

Result Code	Meaning
3	Unknown username or invalid password
4+	Internal error—authentication not processed

The SQL procedure can decide among 1, 2, or 3 to indicate a failure, depending on how much information you want the failed authentication log files to include.

A return code of 4 or higher results in an authentication error event. These errors do not increment per-user failed attempt counters. Additionally, error codes are returned to the AAA client so it can distinguish between errors and failures and, if configured to do so, fall back to a backup AAA server.

Successful or failed authentications are not logged; general Cisco Secure ACS logging mechanisms apply. In the event of an error (CSNTresult equal to or less than 4), the contents of the CSNTerrorString are written to the Windows NT/2000 Event Log under the Application Log.

Configuring a System Data Source Name for an ODBC External User Database

On the Cisco Secure ACS server, you must create a system DSN for Cisco Secure ACS to communicate with the relational database.

To create a system DSN for use with an ODBC external user database, follow these steps:

Step 1 In Windows Control Panel, double-click the **ODBC Data Sources** icon.

Step 2 In the ODBC Data Source Administrator window, click the **System DSN** tab.

Step 3 Click **Add**.

Step 4 Select the driver you need to use with your new DSN, and then click **Finish**.

Result: A dialog box displays fields requiring information specific to the ODBC driver you selected.

Downloaded from www.Manualslib.com manuals search engine

Step 5 Type a descriptive name for the DSN in the Data Source Name box.

Step 6 Complete the other fields required by the ODBC driver you selected. These fields may include information such as the IP address of the server on which the ODBC-compliant database runs.

Step 7 Click **OK**.

Result: The name you assigned to the DSN appears in the System Data Sources list.

Step 8 Close the ODBC window and Windows Control Panel.

Result: The System DSN to be used by Cisco Secure ACS for communication with the relational database is created on your Cisco Secure ACS server.

Configuring an ODBC External User Database

Creating an ODBC database configuration is a process that provides Cisco Secure ACS information that enables it to pass authentication requests to an ODBC-compliant relational database. This information reflects the way you have implemented your relational database and does not dictate how your relational database is configured or functions. For information about your relational database, refer to your relational documentation.

Note Before performing this procedure, you should have completed the steps in the "Preparing to Authenticate Users with an ODBC-Compliant Relational Database" section on page 11-32.

To configure Cisco Secure ACS for ODBC authentication, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

Result: Cisco Secure ACS displays a list of all possible external user database types.

Step 3 Click **External ODBC Database**.

Downloaded from www.Manualslib.com manuals search engine

Step 4 If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for ODBC authentication in the box provided, or accept the default name in the box.

c. Click **Submit**.

Result: Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

Step 5 Click **Configure**.

Step 6 From the System DSN list, select the DSN that is configured on the Cisco Secure ACS server to communicate with the ODBC-compliant relational database you want to use.

Note If you have not configured on the Cisco Secure ACS server a DSN for the relational database, do so before completing these steps. For more information about creating a DSN for Cisco Secure ACS ODBC authentication, see the "Configuring a System Data Source Name for an ODBC External User Database" section on page 11-40.

Step 7 In the DSN Username box, type the username required to perform transactions with your ODBC database.

Step 8 In the DSN Password box, type the password required to perform transactions with your ODBC database.

Step 9 In the DSN Connection Retries box, type the number of times Cisco Secure ACS should try to connect to the ODBC database before timing out. The default is 3.

Note If you have connection problems when Windows NT/2000 starts, increase this value.

Step 10 To change the ODBC worker thread count, in the ODBC Worker Threads box, type the number of ODBC worker threads. The maximum thread count is 10. The default is 1.

Downloaded from www.Manualslib.com manuals search engine

Note Increase the ODBC worker thread count only if the ODBC driver you are using is certified thread safe. For example, the Microsoft Access ODBC driver is not thread safe and can cause Cisco Secure ACS to become unstable if multiple threads are used. Where possible, Cisco Secure ACS queries the driver to find out if it is thread safe. The thread count to use is a factor of how long the DSN takes to execute the procedure and the rate at which authentications are required.

Step 11 From the DSN Procedure Type list, select the type of output your relational database provides. Different databases return different output:

- **Returns Recordset—**The database returns a raw record set in response to an ODBC query. Microsoft SQL Server responds in this manner.
- **Returns Parameters—**The database returns a set of named parameters in response to an ODBC query. Oracle databases respond in this manner.

Step 12 To support PAP authentication with the ODBC database, follow these steps:

a. Select the **Support PAP authentication** check box.

b. In the PAP SQL Procedure box, type the name of the PAP SQL procedure routine that runs on the ODBC server. The default value in this box is CSNTAuthUserPap. If you named the PAP SQL procedure something else, change this entry to match the name given to the PAP SQL procedure. For more information and an example routine, see the "Sample Routine for Generating a PAP Authentication SQL Procedure" section on page 11-35.

Note If you enabled PAP authentication, the PAP authentication SQL procedure must exist on the ODBC database and must have the exact name specified in the PAP SQL Procedure box. If it does not, be sure to create it in the ODBC database before attempting to authenticate users against the ODBC database.

Step 13 To support CHAP authentication with the ODBC database, follow these steps:

a. Select the **Support CHAP/MS-CHAP/ARAP Authentication** check box.

b. In the CHAP SQL Procedure box, type the name of the CHAP SQL procedure routine on the ODBC server. The default value in this box is CSNTExtractUserClearTextPw. If you named the CHAP SQL procedure something else, change this entry to match the name given to the CHAP SQL

Downloaded from www.Manualslib.com manuals search engine

procedure. For more information and an example routine, see the "Sample Routine for Generating an SQL CHAP Authentication Procedure" section on page 11-36.

Note If you enabled CHAP/MS-CHAP/ARAP authentication, the CHAP authentication SQL procedure must exist on the ODBC database and must have the exact name specified in the PAP SQL Procedure box. If it does not, be sure to create it in the ODBC database before attempting to authenticate users against the ODBC database.

Step 14 Click **Submit**.

Result: Cisco Secure ACS saves the ODBC configuration you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see the "Unknown User Processing" section on page 12-1. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "Setting Up and Managing User Accounts."

LEAP Proxy RADIUS Server Database

For Cisco Secure ACS-authenticated users accessing your network via Cisco Aironet devices, Cisco Secure ACS supports MS-CHAP and EAP-TLS authentication with a proxy RADIUS server. Cisco Secure ACS uses MS-CHAP version 1 for LEAP Proxy RADIUS Server authentication. To manage your proxy RADIUS database, refer to your RADIUS database documentation.

Lightweight extensible authentication protocol (LEAP) proxy RADIUS server authentication allows you to authenticate users against existing Kerberos databases that support MS-CHAP authentication. You can use the LEAP Proxy RADIUS Server database to authenticate users with any third-party RADIUS server that supports MS-CHAP authentication.

Downloaded from www.Manualslib.com manuals search engine

Note The third-party RADIUS server must return Microsoft Point-to-Point Encryption (MPPE) keys in the Microsoft RADIUS vendor-specific attribute (VSA) MSCHAP-MPPE-Keys (VSA 12). If the third-party RADIUS server does not return the MPPE keys, the authentication fails and is logged in the Failed Attempts log.

Cisco Secure ACS support RADIUS-based group mapping for users authenticated by LEAP Proxy RADIUS Server databases. For more information, see the "RADIUS-Based Group Specification" section on page 12-21.

Configuring a LEAP Proxy RADIUS Server External User Database

You should install and configure your proxy RADIUS server before configuring Cisco Secure ACS to authenticate users with it. For information about installing the proxy RADIUS server, refer to the documentation included with your RADIUS server.

To configure LEAP proxy RADIUS authentication, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

Result: Cisco Secure ACS displays a list of all possible external user database types.

Step 3 Click **LEAP Proxy RADIUS Server**.

Result: If no LEAP Proxy RADIUS Server configuration exists, only the Database Configuration Creation table appears. Otherwise, in addition to the Database Configuration Creation table, the External User Database Configuration table appears.

Downloaded from www.Manualslib.com manuals search engine

Step 4 If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for the LEAP Proxy RADIUS Server in the box provided, or accept the default name in the box.

c. Click **Submit**.

Result: Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

Step 5 Under External User Database Configuration, select the name of the LDAP database you need to configure.

Note If only one LEAP Proxy RADIUS Server configuration exists, the name of that configuration appears instead of the list. Proceed to the next step.

Step 6 Click **Configure**.

Step 7 In the following boxes, type the required information:

- **Primary Server Name/IP—**IP address of the primary proxy RADIUS server.
- **Secondary Server Name/IP—**IP address of the secondary proxy RADIUS server.
- **Shared Secret—**The shared secret of the proxy RADIUS server. This must be identical to the shared secret with which the proxy RADIUS server is configured.
- **Authentication Port—**The TCP port over which the proxy RADIUS server conducts authentication sessions. If the LEAP Proxy RADIUS server is installed on the same Windows NT/2000 server as Cisco Secure ACS, this port should not be the same port used by Cisco Secure ACS for RADIUS authentication. For more information about the ports used by Cisco Secure ACS for RADIUS, see the "RADIUS" section on page 1-6.
- **Timeout (seconds):—**The number of seconds Cisco Secure ACS waits before sending notification to the user that the authentication attempt has timed out.

Downloaded from www.Manualslib.com manuals search engine

- **Retries—**The number of authentication attempts Cisco Secure ACS makes before failing over to the secondary proxy RADIUS server.
- **Failback Retry Delay (minutes)—**The number of minutes after which Cisco Secure ACS attempts authentications using a failed primary proxy RADIUS server.

Note If both the primary and the secondary servers fail, Cisco Secure ACS alternates between both servers until one responds.

Step 8 Click **Submit**.

Result: Cisco Secure ACS saves the proxy RADIUS token server database configuration you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see the "Unknown User Processing" section on page 12-1. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "Setting Up and Managing User Accounts."

Token Server User Databases

Cisco Secure ACS supports the use of token servers for the increased security provided by one-time passwords (OTPs). This section includes the following topics:

- About Token Servers and Cisco Secure ACS, page 11-48
- About Token Servers and Cisco Secure ACS, page 11-48
- RADIUS-Enabled Token Servers, page 11-49
- Token Servers with Vendor-Proprietary Interfaces, page 11-53

Downloaded from www.Manualslib.com manuals search engine

About Token Servers and Cisco Secure ACS

Cisco Secure ACS provides PAP authentication using token servers. Requests from the access device are first sent to Cisco Secure ACS. If Cisco Secure ACS has been configured to authenticate against a token server and finds the username, it forwards the authentication request to the token server. If it does not find the username, Cisco Secure ACS checks the database configured to authenticate unknown users. If the request for authentication is passed, the appropriate authorizations are forwarded to the access device along with the approved authentication. Cisco Secure ACS then maintains the accounting information.

Cisco Secure ACS acts as a client to the token server. For the token servers supported, Cisco Secure ACS accomplishes this in one of two ways. The first method uses the token server's RADIUS interface. For more information about Cisco Secure ACS support of token servers with a RADIUS interface, see the "RADIUS-Enabled Token Servers" section on page 11-49.

For some token servers, Cisco Secure ACS uses the token server vendor's proprietary API. For more information about Cisco Secure ACS support of token servers using the token server vendor's proprietary API, see the "Token Servers with Vendor-Proprietary Interfaces" section on page 11-53.

Token Servers and ISDN

Cisco Secure ACS supports token caching for ISDN terminal adapters and routers. One inconvenience of using token cards for OTP authentication with ISDN is that each B channel requires its own OTP. Therefore, a user must enter at least 2 OTPs, plus any other login passwords, such as those for Windows NT/2000 networking. If the terminal adapter supports the ability to turn on and off the second B channel, users might have to enter many OTPs each time the second B channel comes into service.

Cisco Secure ACS caches the token to help make the OTPs easier for users. This means that if a token card is being used to authenticate a user on the first B channel, a specified period can be set during which the second B channel can come into service without requiring the user to enter another OTP. To lessen the risk of unauthorized access to the second B channel, you can limit the time the second B channel is up. Furthermore, you can configure the second B channel to use the CHAP password specified during the first login to further lessen the chance of a security problem. When the first B channel is dropped, the cached token is erased.

Downloaded from www.Manualslib.com manuals search engine

RADIUS-Enabled Token Servers

This section describes Cisco Secure ACS support for token servers that provide a standard RADIUS interface.

About RADIUS-Enabled Token Servers

Cisco Secure ACS can support token servers using the RADIUS server built into the token server. Rather than using the vendor's proprietary API, Cisco Secure ACS sends standard RADIUS authentication requests to the RADIUS authentication port on the token server. The token servers supported through their RADIUS servers are as follows:

- ActivCard
- CRYPTOCard
- Vasco

You can create multiple instances of each of these token server types in Cisco Secure ACS. For information about configuring Cisco Secure ACS to authenticate users with one of these token servers, see the "Configuring a RADIUS Token Server External User Database" section on page 11-50.

Cisco Secure ACS also supports any token server that is a RADIUS server compliant with IETF RFC 2865. So, in addition to the RADIUS-enabled token server vendors explicitly supported, this enables you to use any token server that supports RADIUS-based authentication.

Although Cisco Secure ACS supports mapping users authenticated by a RADIUS-enabled token server to a single group, Cisco Secure ACS also provides a means for specifying a user's group assignment in the RADIUS response from the RADIUS-enabled token server. For more information, see the "RADIUS-Based Group Specification" section on page 12-21.

Downloaded from www.Manualslib.com manuals search engine

Token Server RADIUS Authentication Request and Response Contents

When Cisco Secure ACS forwards an authentication request to a RADIUS-enabled token server, the RADIUS authentication request contains the following attributes:

- User-Name (RADIUS attribute 1)
- User-Password (RADIUS attribute 2)
- NAS-IP-Address (RADIUS attribute 4)
- NAS-Port (RADIUS attribute 5)
- NAS-Identifier (RADIUS attribute 32)

Cisco Secure ACS expects to receive one following three responses:

- **access-accept**—No attributes are required; however, the response can indicate the Cisco Secure ACS group to which the user should be assigned. For more information, see the "RADIUS-Based Group Specification" section on page 12-21.
- **access-reject**—No attributes required.
- **access-challenge—**Attributes required, per IETF RFC, are as follows:
- State (RADIUS attribute 24)
- Reply-Message (RADIUS attribute 18)

Configuring a RADIUS Token Server External User Database

Use this procedure to configure ActivCard, CRYPTOCard, Vasco, and RADIUS Token Server external user databases in Cisco Secure ACS.

Before You Begin

You should install and configure your RADIUS token server before configuring Cisco Secure ACS to authenticate users with it. For information about installing the RADIUS token server, refer to the documentation included with your token server.

Downloaded from www.Manualslib.com manuals search engine

To configure Cisco Secure ACS to authenticate users with a ActivCard token server, CRYPTOCard token server, Vasco token server, or generic RADIUS Token Sever, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

Result: Cisco Secure ACS displays a list of all possible external user database types. The external user databases that represent RADIUS-enabled token servers are as follows:

- ActivCard
- CRYPTOCard
- RADIUS Token Server
- Vasco

Step 3 Click the link for the applicable RADIUS-enabled token server.

Result: The Database Configuration Creation table appears. If at least one configuration exists for the selected external user database type, the External User Database Configuration table also appears.

Step 4 If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for the RADIUS-enabled token server in the box provided, or accept the default name in the box.

c. Click **Submit**.

Result: Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

Step 5 Under External User Database Configuration, select the name of the RADIUS-enabled token server you need to configure.

Note If only one RADIUS-enabled token server configuration exists, the name of that configuration appears instead of the list. Continue with Step 6.

Downloaded from www.Manualslib.com manuals search engine

Step 6 Click **Configure**.

Step 7 In the following boxes, type the required information:

- **Primary Server Name/IP—**The hostname or IP address of the primary RADIUS token server. If you provide the hostname, the hostname must be resolvable by DNS.
- **Secondary Server Name/IP—**The hostname or IP address of the secondary RADIUS token server. If you provide the hostname, the hostname must be resolvable by DNS.
- **Shared Secret—**The shared secret of the RADIUS server. This must be identical to the shared secret with which the RADIUS token server is configured.
- **Authentication Port—**The TCP port over which the RADIUS server conducts authentication sessions. If the RADIUS token server is installed on the same Windows NT/2000 server as Cisco Secure ACS, this port should not be the same port used by Cisco Secure ACS for RADIUS authentication. For more information about the ports used by Cisco Secure ACS for RADIUS, see the "RADIUS" section on page 1-6.
- **Timeout (seconds):—**The number of seconds Cisco Secure ACS waits for a response from the RADIUS token server before retrying the authentication request.
- **Retries—**The number of authentication attempts Cisco Secure ACS makes before failing over to the secondary RADIUS token server.
- **Failback Retry Delay (minutes)—**The number of minutes that Cisco Secure ACS sends authentication requests to the secondary server when the primary server has failed. When this duration is ended, Cisco Secure ACS reverts to sending authentication requests to the primary server.

Note If both the primary and the secondary servers fail, Cisco Secure ACS alternates between both servers until one responds.

Downloaded from www.Manualslib.com manuals search engine

Step 8 Click **Submit**.

Result: Cisco Secure ACS saves the RADIUS token server database configuration you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see the "Unknown User Processing" section on page 12-1. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "Setting Up and Managing User Accounts."

Token Servers with Vendor-Proprietary Interfaces

Cisco Secure ACS supports several token servers by communicating via the token server vendor's proprietary API.

About Token Servers with Proprietary Interfaces

For token servers supported by using the token server vendor's proprietary API, Cisco Secure ACS acts as a token-card client to the token server. In some cases, this means that the token-card client software is installed on the Cisco Secure ACS server. In others, you must provide Cisco Secure ACS with information about the token server. The token servers supported through their vendor's proprietary API are as follows:

- **RSA SecurID**—Cisco Secure ACS supports PPP (ISDN and async) and Telnet for RSA SecurID.
- **SafeWord**—Cisco Secure ACS supports PPP (ISDN and async) and Telnet for SafeWord.
- **AXENT**—Cisco Secure ACS supports PPP (over async only) and Telnet for AXENT, not PPP with ISDN.

Configuring a SafeWord Token Server External User Database

Cisco Secure ACS supports the SafeWord token server custom interface for authentication of users. You can create only one SafeWord configuration within Cisco Secure ACS.

Downloaded from www.Manualslib.com manuals search engine

Before You Begin

You should install and configure your SafeWord token server before configuring Cisco Secure ACS to authenticate users with it. For information about installing the SafeWord server, refer to the documentation included with your token server.

To configure Cisco Secure ACS to authenticate users with a SafeWord token server, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

Result: Cisco Secure ACS displays a list of all possible external user database types.

Step 3 Click **SafeWord Token Server**.

Result: If no SafeWord token server configuration exists, the Database Configuration Creation table appears. Otherwise, the External User Database Configuration page appears.

Step 4 If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for the SafeWord token server in the box provided, or accept the default name in the box.

c. Click **Submit**.

Result: Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

Step 5 Click **Configure**.

Step 6 In the following boxes, type the required information:

- **Server Name—**Mnemonic for the user, preferably the name of the remote sever.
- **Server Address—**The IP address of the SafeWord token server.

Downloaded from www.Manualslib.com manuals search engine

Step 7 Click **Submit**.

Result: Cisco Secure ACS saves the SafeWord token server database configuration you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see the "Unknown User Processing" section on page 12-1. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "Setting Up and Managing User Accounts."

Configuring an AXENT Token Server External User Database AXENT

Cisco Secure ACS supports the AXENT token server custom interface for authentication of users. You can create only one AXENT configuration within Cisco Secure ACS.

Before You Begin

You should install and configure your AXENT token server before configuring Cisco Secure ACS to authenticate users with it. For information about installing the AXENT server, refer to the documentation included with your token server.

To configure Cisco Secure ACS to authenticate users with an AXENT token server, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

Result: Cisco Secure ACS displays a list of all possible external user database types.

Step 3 Click **AXENT Token Server**.

Result: If no AXENT token server configuration exists, the Database Configuration Creation table appears. Otherwise, the External User Database Configuration page appears.

Downloaded from www.Manualslib.com manuals search engine

Step 4 If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for the AXENT token server in the box provided, or accept the default name in the box.

c. Click **Submit**.

Result: Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

Step 5 Click **Configure**.

Step 6 In the following boxes, type the required information:

- **Server Name—**Name of the defender security server.
- **Server Address—**IP address of the defender security server.
- **Server Port—**Port number of the defender security server.
- **Communication Timeout—**Number of seconds to wait before sending notification to the user that the connection has timed out.
- **Agent ID—**Identification of an agent that has been approved by the server.
- **Agent Key—**Agent's SNK key in hexadecimal numbers (00 to FF).

Step 7 Click **Submit**.

Result: Cisco Secure ACS saves the AXENT token server database configuration you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see the "Unknown User Processing" section on page 12-1. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "Setting Up and Managing User Accounts."

Configuring an RSA SecurID Token Server External User Database

Cisco Secure ACS supports the RSA SecurID token server custom interface for authentication of users. You can create only one RSA SecurID configuration within Cisco Secure ACS.

Downloaded from www.Manualslib.com manuals search engine

Before You Begin

You should install and configure your RSA SecurID token server before configuring Cisco Secure ACS to authenticate users with it. For information about installing the RSA SecurID server, refer to the documentation included with your token server.

To configure Cisco Secure ACS to authenticate users with an RSA token server, follow these steps:

Step 1 Install the RSA client on the Cisco Secure ACS server:

a. Before you begin:

- Log in to the Windows NT/2000 server with administrative privileges.
- Make sure you have the ACE Client for Windows NT/2000 software.

b. Run the Setup program of the ACE Client software (following the setup instructions). Do not restart your Windows NT/2000 server when installation is complete.

c. Locate the ACE Server data directory, for example, `/sdi/ace/data`.

d. Get the file named `sdconf.rec` and place it in your Windows NT directory:

```
%SystemRoot%\system32
```

For example:

```
\winnt\system32
```

e. Make sure the ACE server host machine name is in the Windows NT/2000 local host's file:

`\`*Windows directory*`\system32\drivers\etc\hosts`

f. Restart your Windows NT/2000 server.

g. Verify connectivity by running the Test Authentication function of your ACE client application. You can run this from Control Panel.

Step 2 In the navigation bar, click **External User Databases**.

Step 3 Click **Database Configuration**.

Result: Cisco Secure ACS displays a list of all possible external user database types.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Click **RSA SecurID Token Server**.

Result: If no RSA SecurID token server configuration exists, the Database Configuration Creation table appears. Otherwise, the External User Database Configuration page appears.

Step 5 If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for the RSA SecurID token server in the box provided, or accept the default name in the box.

c. Click **Submit**.

Result: Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

Step 6 Click **Configure**.

Result: Cisco Secure ACS displays the name of the token server and the path to the authenticator DLL. This information confirms that Cisco Secure ACS can contact the RSA client. You can add the RSA SecurID external user database to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see the "Unknown User Processing" section on page 12-1. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "Setting Up and Managing User Accounts."

Deleting an External User Database Configuration

If you no longer need a particular external user database configuration, you can delete it from Cisco Secure ACS.

To delete an external user database configuration, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

Result: Cisco Secure ACS displays a list of all possible external user database types.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Click the external user database type for which you want to delete a configuration.

Result: The External User Database Configuration table appears.

Step 4 If a list appears in the External User Database Configuration table, select the configuration you want to delete. Otherwise, proceed to the next step.

Step 5 Click **Delete**.

Result: A confirmation dialog box appears.

Step 6 Click **OK** to confirm that you want to delete the external user database configuration.

Result: The external user database configuration you selected is deleted from Cisco Secure ACS.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Administering External User Databases

After you have configured Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) to communicate with an external user database, you can decide how to implement other Cisco Secure ACS features related to external user databases. To address these features, this chapter contains the following sections:

- Unknown User Processing, page 12-1
- Database Group Mappings, page 12-10

For information about the databases supported by Cisco Secure ACS and how to configure Cisco Secure ACS to communicate with an external user database, see Chapter 11, “Working with User Databases.”

Unknown User Processing

Unknown users are users who are not listed in the Cisco Secure ACS database. The Unknown User feature is a form of authentication forwarding. In essence, this feature is an extra step in the authentication process. In this additional step of the authentication process, if the username does not exist in the Cisco Secure ACS database, Cisco Secure ACS forwards the authentication request of an incoming username and password to external databases with which it is configured to communicate.

Downloaded from www.Manualslib.com manuals search engine

The Unknown User feature enables Cisco Secure ACS to use a variety of external databases in addition to its own internal database to authenticate incoming user requests. With this feature, Cisco Secure ACS provides the foundation for a basic single sign-on capability by integrating network and host-level access control. Because the incoming usernames and passwords of users dialing in can be authenticated with external user databases, there is no need for the network administrator to maintain a duplicate list within Cisco Secure ACS. This provides two advantages to the Cisco Secure ACS administrator:

- Eliminates the necessity of entering every user multiple times
- Prevents data-entry errors that are inherent to manual procedures

Known, Unknown, and Cached Users

The Unknown User feature implements three categories of users in Cisco Secure ACS. Each category is treated differently:

- **Known Users** explicitly added, either manually or automatically, into the Cisco Secure ACS database.

  These are users added through User Setup in the HTML interface, by the RDBMS Synchronization feature, by the Database Replication feature, or through by the CSUtil.exe utility. For more information about **CSUtil.exe**, see Appendix E, "Cisco Secure ACS Command-Line Database Utility." In the CiscoSecure user database, each user must have an assigned password and must be explicitly associated with a particular authentication database.

- **Unknown Users**—Users who have no account entry in the CiscoSecure user database.

  Such users never have previously authenticated with Cisco Secure ACS. If the Unknown User Policy is configured in Cisco Secure ACS, Cisco Secure ACS attempts to authenticate these users with external user databases.

- **Cached Users—**Users whose accounts were automatically added to the Cisco Secure ACS database when Cisco Secure ACS successfully authenticated them using the Unknown User Policy.

  All cached users were once unknown users. The authentication process for cached users is identical to the authentication process for known users.

Downloaded from www.Manualslib.com manuals search engine

General Authentication Request Handling and Rejection Mode

If you have configured the Unknown User Policy in Cisco Secure ACS, Cisco Secure ACS attempts to authenticate users as follows:

1. Cisco Secure ACS checks its internal user database. If the user exists in the CiscoSecure user database (that is, is a known or cached user), Cisco Secure ACS tries to authenticate the user with the specified password type against the specified database. Authentication for that user either passes or fails, depending on other procedures in the normal authentication process.
2. If the user does not exist in the CiscoSecure user database (that is, is an unknown user), Cisco Secure ACS tries each configured external database in the order specified in the Selected Databases list. If the user passes authentication against one of the external databases, Cisco Secure ACS automatically adds the user to the CiscoSecure user database, with a pointer to use the password type and database that succeeded on this authentication attempt. Users added by unknown user processing are flagged as such within the CiscoSecure user database and are called cached users.

   The next time the cached user tries to authenticate, Cisco Secure ACS authenticates the user against the database that was successful the first time. Cached users are treated the same as known users.
3. If the unknown user fails authentication with all configured external databases, the user is not added to the CiscoSecure user database, and the authentication request is rejected.

Because usernames in the CiscoSecure user database must be unique, Cisco Secure ACS supports a single instance of any given username across all the databases it is configured to use. For example, assume every external user database contains a user account with the username John. Each account is for a different user, but they each, coincidentally, have the same exact username. After the first John attempts to access the network and has authenticated through the unknown user process, Cisco Secure ACS retains a cached user account for that John and only that John. Now, Cisco Secure ACS tries to authenticate subsequent attempts by any user named John using the same external user database that originally authenticated John. Assuming their passwords are different than the password for the John who authenticated first, the other Johns are unable to access the network.

Downloaded from www.Manualslib.com manuals search engine

Note The scenario given above is handled differently if the user accounts with identical usernames exist in separate Windows domains. For more information, see the "Authentication Request Handling and Rejection Mode with the Windows NT/2000 User Database" section on page 12-4.

Authentication Request Handling and Rejection Mode with the Windows NT/2000 User Database

Because it is a native Windows NT/2000 application, Cisco Secure ACS treats authentication with a Windows NT/2000 user database as a special case. Windows can provide added functionality to the remote access authentication process. Perhaps the most important aspect of this added functionality is support for multiple occurrences of the same username across the trusted domains against which Cisco Secure ACS authenticates access requests.

Cisco Secure ACS communicates with the Windows NT/2000 operating system of the Cisco Secure ACS server to perform authentications. Windows NT/2000 uses its built-in facilities to forward the authentication requests to the appropriate domain controller. There are two possible scenarios to consider:

- Authentication requests in which the domain name is supplied
- Authentication requests in which the domain name is omitted

Windows Authentication with a Domain Specified

When a domain name is supplied as part of a authentication request, Cisco Secure ACS detects that a domain name was supplied and tries the authentication credentials against the specified domain. The dial-up networking client provided with Window NT/2000 and Windows 95/98 differ in the method by which users can specify their domains. For more information, see the "Windows Dial-up Networking Clients" section on page 11-9.

If the domain controller rejects the authentication request, Cisco Secure ACS logs the request as a failed attempt.

Specifying the domain name allows Cisco Secure ACS to differentiate a user from multiple instances of the same username in different domains. For unknown users who provide a domain name and who are authenticated by a Windows

Downloaded from www.Manualslib.com manuals search engine

NT/2000 database, Cisco Secure ACS caches the username in the CiscoSecure user database in the form *domain\user*. The combination of username and domain makes this cached user unique in the Cisco Secure ACS database.

Note Cisco Secure ACS does not support the *user@domain* form of qualified usernames.

Note We recommend removing a username from a database when the privileges associated with that username are no longer required.

Windows Authentication with Domain Omitted

If the appropriate domain identifier is not supplied as part of the authentication process, as with the Windows 95/98 dial-up networking client or with Windows NT/2000 in a workgroup environment, the Windows NT/2000 operating system of the Cisco Secure ACS server follows a more complex authentication process. It first attempts to authenticate the user against its local domain controller. If the user does not exist in the local domain controller's user database, it progresses down the list of all its trusted domains, trying the username against each one. If Windows NT/2000 does not find the username, it tries the credentials against its local accounts database. If it does not find the username in the local accounts database, it rejects the authentication request. If authentication succeeds against the local domain, any of the trusted domains, or the local Windows NT/2000 accounts database, the user is granted access and Cisco Secure ACS ceases further attempts to find the user in other domains.

If the username exists in the local domain or any of the trusted domains but the password does not match the one supplied as part of the authentication credentials, Windows NT/2000 returns a rejection message to Cisco Secure ACS. You can circumvent this difficulty by using the Domain List in the Cisco Secure ACS configuration for the Windows NT/2000 database. If you have configured the Domain List with a list of trusted domains, Cisco Secure ACS submits the username and password to each domain in the list, using a domain-qualified format, until Cisco Secure ACS successfully authenticates the user. If Cisco Secure ACS has tried each domain listed in the Domain List, or if no trusted domains have been configured in the Domain List, Cisco Secure ACS fails the authentication request for that user.

Downloaded from www.Manualslib.com manuals search engine

Note If your network has multiple occurrences of a username across domains (for example, every domain has a user called Administrator) or if users dialing in do not provide their domains as part of their authentication credentials, be sure to configure the Domain List for the Windows NT/2000 database in the External User Databases section. If not, only the user whose account Windows NT/2000 happens to check first authenticates successfully. The Domain List is the only way that Cisco Secure ACS controls the order in which Windows NT/2000 checks domains. The most reliable method of supporting multiple instances of a username across domains is to require users to supply their domain memberships as part of the authentication request.

Performance of Unknown User Authentication

Authentication requests that use the Unknown User authentication feature require slightly more time. This small delay may require additional configuration on the AAA clients through which unknown users may attempt to access your network.

Added Latency

Adding external databases against which to process unknown users can significantly increase the time needed for each individual authentication. At best, the time needed for each authentication is the time taken by the external database to authenticate, plus some latency for Cisco Secure ACS processing. In some circumstances (for example, when using a Windows NT/2000 user database), the extra latency introduced by an external database can be as much as tens of seconds. If you have configured multiple databases, this number is multiplied by the time taken for each one to complete.

Authentication Timeout Value on AAA clients

Be sure to increase the AAA client timeout to accommodate the longer authentication time required for Cisco Secure ACS to pass the authentication request to the external databases. If the AAA client timeout value is not set high enough to account for the delay required by unknown user authentication, the AAA client times out the request and every unknown user authentication fails.

Downloaded from www.Manualslib.com manuals search engine

The default AAA client timeout value is 5 seconds. If you have Cisco Secure ACS configured to search through several databases or if your databases are large, you might need to increase this value in your AAA client configuration file. For more information, refer to your Cisco IOS documentation.

Network Access Authorization

While the Unknown User Policy allows authentication requests to be forwarded to external user databases, all responsibility for the authorization parameters provided to the AAA client remains with Cisco Secure ACS. External user databases provide authentication services, and Cisco Secure ACS then provides the additional authorization information that is sent to the AAA client in the RADIUS or TACACS+ response packet. For more information about assignment of user authorization, see the "Database Group Mappings" section on page 12-10.

Unknown User Policy

You can configure how Cisco Secure ACS processes unknown users on the Configure Unknown User Policy page, in the External User Databases section of the HTML interface. The Configure Unknown User Policy page contains the following fields:

- **Unknown User Policy—**Defines what action Cisco Secure ACS takes if it does not find a matching username in its database. There are two options for controlling the Unknown User Policy:
  - **Fail the attempt—**Disables unknown user processing. Cisco Secure ACS rejects authentication requests for any user not found in the CiscoSecure user database.
  - **Check the following external user databases—**Enables unknown user processing. Cisco Secure ACS uses databases in the Selected Databases list to authenticate users that are not found in the CiscoSecure user database.
- **External Databases—**Lists the external user databases that Cisco Secure ACS does *not* use to authenticate unknown users.
- **Selected Databases—**Lists the external user databases Cisco Secure ACS that uses to authenticate an unknown user (if the Check the following external user databases option is selected). Cisco Secure ACS attempts authentication

Downloaded from www.Manualslib.com manuals search engine

using the selected databases serially and in the order specified, top to bottom. For more information about the significance of the order of selected databases, see the "Database Search Order" section on page 12-8.

For more information about configuring your Unknown User Policy, see the "Configuring the Unknown User Policy" section on page 12-8

Database Search Order

You can configure the order in which Cisco Secure ACS checks the selected external databases when Cisco Secure ACS attempts to authenticate unknown users. If the first database in the Selected Databases list fails the authentication request for the unknown user, Cisco Secure ACS checks the next database listed, and so on down the Selected Databases list, in the order listed, until the user authenticates or until Cisco Secure ACS has tried all the databases listed. Authentication with a Windows NT/2000 database is more complex. (For more information about Windows NT/2000 authentication, see the "The Cisco Secure ACS Authentication Process with Windows NT/2000 User Databases" section on page 11-7.) If Cisco Secure ACS does not find the user in any of the listed databases, authentication fails.

The order in which the databases appear in the Selected Databases list is important. For best performance, authentications should be processed first against the external database where the greatest number of authentications are likely to succeed (that is, get the highest level of successful cache hits).

Tip Always list the database that will allow most authentications to succeed as near to the top of the list as possible.

Configuring the Unknown User Policy

In Cisco Secure ACS, an unknown user is defined as one for whom no account has been created within the Cisco Secure ACS database.

To specify how Cisco Secure ACS should handle users who are not in the Cisco Secure ACS database, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Unknown User Policy**.

Downloaded from www.Manualslib.com manuals search engine

Step 3 To deny authentication requests for any unknown user, select the **Fail the attempt** option.

Step 4 To allow authentication requests for unknown users, follow these steps:

a. Select the **Check the following external user databases** option.

b. For each database you need Cisco Secure ACS to use when attempting to authenticate unknown users, select the database in the External Databases list and click —> (right arrow button) to move it to the Selected Databases list. To remove a database from the Selected Databases list, select the database, and then click <— (left arrow button) to move it back to the External Databases list.

c. To assign the order in which Cisco Secure ACS should use the selected external databases when attempting to authenticate an unknown user, click a database name in the Selected Databases list and click **Up** or **Down** to move it into the position you want.

d. Repeat Steps a through c until the selected databases are in the order needed.

Step 5 Click **Submit**.

Result: Cisco Secure ACS saves and implements the Unknown User Policy configuration you created. Cisco Secure ACS attempts to authenticate unknown users using the databases in the order listed in the Selected Databases list.

Turning off External User Database Authentication

You can configure Cisco Secure ACS so that users who are not in the Cisco Secure ACS database are not permitted to authenticate.

To turn off external user database authentication, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Unknown User Policy**.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select the **Fail the attempt** option.

Step 4 Click **Submit**.

Result: Unknown user processing is halted. Cisco Secure ACS does not allow unknown users to authenticate with external user databases.

Database Group Mappings

The Database Group Mapping feature in the External User Databases section enables you to associate unknown users with a Cisco Secure ACS group for the purposes of assigning authorization profiles. For external user databases from which Cisco Secure ACS can derive group information, you can associate the group memberships defined for the users in the external user database to specific Cisco Secure ACS groups. For Windows NT/2000 user databases, group mapping is further specified by domain, because each domain maintains its own user database. For Novell NDS user databases, group mapping is further specified by tree, because Cisco Secure ACS supports multiple trees in a single Novell NDS user database.

In addition to the Database Group Mapping feature, for some database types, Cisco Secure ACS supports RADIUS-based group specification.

This section contains the following topics:

- Group Mapping by External User Database, page 12-10
- Group Mapping by Group Set Membership, page 12-13
- RADIUS-Based Group Specification, page 12-21

Group Mapping by External User Database

You can map an external database to a Cisco Secure ACS group. Unknown users who authenticate using the specified database automatically belong to, and inherit the authorizations of, the group. For example, you could configure Cisco Secure ACS so that all unknown users who authenticate with a certain token server database belong to a group called Telecommuters. You could then

Downloaded from www.Manualslib.com manuals search engine

assign a group setup that is appropriate for users who are working away from home, such as MaxSessions=1. Or you could configure restricted hours for other groups, but give unrestricted access to Telecommuters group members.

While you can configure Cisco Secure ACS to map all unknown users found in any external user database type to a single Cisco Secure ACS group, the following external user database types are the external user database types whose users you can only map to a single Cisco Secure ACS group:

- ODBC
- LEAP Proxy RADIUS server
- ActivCard token server
- AXENT token server
- CRYPTOCard token server
- RADIUS token server
- RSA SecurID token server
- SafeWord token server
- Vasco token server

For a subset of the external user database types listed above, group mapping by external database type is overridden on a user-by-user basis when the external user database specifies a Cisco Secure ACS group with its authentication response. Cisco Secure ACS supports specification of group membership for the following external user database types:

- LEAP Proxy RADIUS server
- ActivCard token server
- CRYPTOCard token server
- RADIUS token server
- Vasco token server

For more information about specifying group membership for users authenticated with one of these database types, see the "RADIUS-Based Group Specification" section on page 12-21.

Downloaded from www.Manualslib.com manuals search engine

Additionally, users authenticated by an ODBC external user database can also be assigned to a specified Cisco Secure ACS group. Group specification by ODBC database authentication overrides group mapping. For more information about specifying group membership for users authenticated with an ODBC database, see the "ODBC Database" section on page 11-30.

Creating a Cisco Secure ACS Group Mapping for a Token Server, ODBC Database, or LEAP Proxy RADIUS Server Database

To set or change a token server, ODBC, or LEAP Proxy RADIUS Server database group mapping, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the name of the token server, LEAP Proxy RADIUS Server, or ODBC database configuration for which you want to configure a group mapping.

Result: The Define Group Mapping table appears.

Step 4 From the Select a default group for *database* list, click the group to which users authenticated with this database should be assigned.

Tip The Select a default group for *database* list displays the number of users assigned to each group.

Step 5 Click **Submit**.

Result: Cisco Secure ACS assigns unknown and cached users authenticated by the external database type you selected in Step 3 to the Cisco Secure ACS group selected in Step 4. For users authenticated by an ODBC, ActivCard, or LEAP Proxy RADIUS Server database, the mapping is only applied as a default if those databases did not specify a Cisco Secure ACS group for the user.

Downloaded from www.Manualslib.com manuals search engine

Group Mapping by Group Set Membership

You can create group mappings for some external user databases based on the combination of external user database groups to which users belong. The following are the external user database types for which you can create group mappings based on group set membership:

- Windows NT/2000
- Novell NDS
- Generic LDAP

Note Windows NT/2000 databases are defined by domain name.

When you configure a Cisco Secure ACS group mapping based on group set membership, you can add one or many external user database groups to the set. For Cisco Secure ACS to map a user to the specified Cisco Secure ACS group, the user must match *all* the external user database groups in the set.

As an example, you could configure a group mapping for users who belong to both the Engineering and Tokyo groups and a separate one for users who belong to both Engineering and London. You could then configure separate group mappings for the combinations of Engineering-Tokyo and Engineering-London and configure different access times for the Cisco Secure ACS groups to which they map. You could also configure a group mapping that only included the Engineering group that would map other members of the Engineering group who were not members of Tokyo or London.

Group Mapping Order

Cisco Secure ACS always maps users to a single Cisco Secure ACS group, yet a user can belong to more than one group set mapping. For example, a user, John, could be a member of the group combination Engineering and California, and at the same time be a member of the group combination Engineering and Managers. If there are Cisco Secure ACS group set mappings for both these combinations, Cisco Secure ACS has to determine to which group John should be assigned.

Cisco Secure ACS prevents conflicting group set mappings by assigning the group set mappings a mapping order. When a user authenticated by an external user database is to be assigned to a Cisco Secure ACS group, Cisco Secure ACS

Downloaded from www.Manualslib.com manuals search engine

starts at the top of the list of group mappings for that database. Cisco Secure ACS checks the user's group memberships in the external user database against each group mapping in the list sequentially. Upon finding the first group set mapping that matches the user's external user database group memberships, Cisco Secure ACS assigns the user to that group mapping's Cisco Secure ACS group and terminates the mapping process.

Clearly, the order of group mappings is important because it affects the network access and services allowed users. When defining mappings for users who belong to multiple groups, make sure they are in the correct order so that users are granted the correct group settings.

For example, a user, Mary, is assigned to the three-group combination of Engineering, Marketing, and Managers. Mary should be granted the privileges of a manager rather than an engineer. Mapping A assigns users who belong to all three of Mary's groups to Cisco Secure ACS Group 2. Mapping B assigns users who belong to the Engineering and Marketing groups to Cisco Secure ACS Group 1. If Mapping B is listed first, Cisco Secure ACS authenticates Mary as a user of Group 1, and she is be assigned to Group 1, rather than Group 2 like managers should be.

No Access Group for Group Set Mappings

To prevent remote access for users assigned a group by a particular group set mapping, assign the group to the Cisco Secure ACS No Access group. For example, you could assign all members of an external user database group "Contractors" to the No Access group so they could not dial in to the network remotely.

Default Group Mapping for Windows NT/2000

For Windows NT/2000 user databases, Cisco Secure ACS includes the ability to define a default group mapping. If no other group mapping matches an unknown user authenticated by a Windows NT/2000 user database, Cisco Secure ACS assigns the user to a group based on the default group mapping.

Configuring the default group mapping for Windows NT/2000 user databases is the same as editing an existing group mapping, with one exception. When editing the default group mapping for Windows NT/2000, instead of selecting a valid domain name on the Domain Configurations page, select \DEFAULT.

Downloaded from www.Manualslib.com manuals search engine

For more information about editing an existing group mapping, see the "Editing a Windows NT/2000, Novell NDS, or Generic LDAP Group Set Mapping" section on page 12-17.

Creating a Cisco Secure ACS Group Mapping for Windows NT/2000, Novell NDS, or Generic LDAP Groups

To map a Windows NT/2000, Novell NDS, or generic LDAP group to a Cisco Secure ACS group, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the external user database name for which you want to configure a group mapping.

Result: If you are mapping a Windows NT/2000 group set, the Domain Configurations table appears. If you are mapping an NDS group set, the NDS Trees table appears. Otherwise, the Group Mappings for *database* Users table appears.

Step 4 If you are mapping a Windows NT/2000 group set for a new domain, follow these steps:

a. Click **New configuration**.

Result: The Define New Domain Configuration page appears.

b. If the Windows domain for which you want to create a group set mapping configuration appears in the Detected domains list, select the name of the domain.

Tip To clear your domain selection, click Clear Selection.

c. If the Windows domain for which you want to create a group set mapping *does not appear* in the Detected domains list, type the name of a trusted Windows NT/2000 domain in the Domain box.

d. Click **Submit**.

Result: The new Windows NT/2000 domain appears in the list of domains in the Domain Configurations page.

Downloaded from www.Manualslib.com manuals search engine

Step 5 If you are mapping a Windows NT/2000 group set, click the domain name for which you want to configure a group set mapping.

Result: The Group Mappings for Domain: *domainname* table appears.

Step 6 If you are mapping a Novell NDS group set, click the name of the Novell NDS tree for which you want to configure group set mappings.

Result: The Group Mappings for NDS Users table appears.

Step 7 Click **Add Mapping**.

Result: The Create new group mapping for *database* page opens. The group list displays group names derived from the external user database.

Step 8 For each group to be added to the group set mapping, select the name of the applicable external user database group in the group list, and then click **Add to selected**.

Note A user must match *all* the groups in the Selected list in order for Cisco Secure ACS to use this group set mapping to map the user to a Cisco Secure ACS group; however, a user can also belong to other groups (in addition to the groups listed) and still be mapped to a Cisco Secure ACS group.

Tip To remove a group from the mapping, select the name of the group in the Selected list, and then click **Remove from selected**.

Result: The Selected list shows all the groups that a user must belong to in order to be mapped to a Cisco Secure ACS group.

Step 9 In the CiscoSecure group list, select the name of the Cisco Secure ACS group to which you want to map users who belong to all the external user database groups in the Selected list.

Note You can also select <No Access>. For more information about the <No Access> group, see the "No Access Group for Group Set Mappings" section on page 12-14.

Downloaded from www.Manualslib.com manuals search engine

Step 10 Click **Submit**.

Result: The group set you mapped to the Cisco Secure ACS list appears at the bottom of the *database* groups column.

Note The asterisk at the end of each set of groups indicates that users authenticated with the external user database can belong to other groups besides those in the set.

Editing a Windows NT/2000, Novell NDS, or Generic LDAP Group Set Mapping

You can change the Cisco Secure ACS group to which a group set mapping is mapped.

Note The external user database groups of an existing group set mapping cannot be edited. If you want to add or remove external user database groups from the group set mapping, delete the group set mapping and create one with the revised set of groups.

To edit a Windows NT/2000, Novell NDS, or generic LDAP group mapping, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the external user database name for which you want to edit a group set mapping.

Result: If you are editing a Windows NT/2000 group set mapping, the Domain Configurations table appears. If you are editing an NDS group set mapping, the NDS Trees table appears. Otherwise, the Group Mappings for *database* Users table appears.

Step 4 If you are editing a Windows NT/2000 group set mapping, click the domain name for which you want to edit a group set mapping.

Result: The Group Mappings for Domain: *domainname* table appears.

Downloaded from www.Manualslib.com manuals search engine

Step 5 If you are editing a Novell NDS group set mapping, click the name of the Novell NDS tree for which you want to edit a group set mapping.

Result: The Group Mappings for NDS Users table appears.

Step 6 Click the group set mapping to be edited.

Result: The Edit mapping for *database* page opens. The external user database group or groups included in the group set mapping appear above the CiscoSecure group list.

Step 7 From the CiscoSecure group list, select the name of the group to which the set of external database groups should be mapped, and then click **Submit**.

Note You can also select <No Access>. For more information about the <No Access> group, see the "No Access Group for Group Set Mappings" section on page 12-14.

Step 8 Click **Submit**.

Result: The Group Mappings for *database* page opens again with the changed group set mapping listed.

Deleting a Windows NT/2000, Novell NDS, or Generic LDAP Group Set Mapping

You can delete individual group set mappings.

To delete a Windows NT/2000, Novell NDS, or generic LDAP group mapping, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the external user database configuration whose group set mapping you need to delete.

Result: If you are deleting a Windows NT/2000 group set mapping, the Domain Configurations table appears. If you are deleting an NDS group set mapping, the NDS Trees table appears. Otherwise, the Group Mappings for *database* Users table appears.

Downloaded from www.Manualslib.com manuals search engine

Step 4 If you are deleting a Windows NT/2000 group set mapping, click the domain name whose group set mapping you want to delete.

Result: The Group Mappings for Domain: *domainname* table appears.

Step 5 If you are deleting a Novell NDS group set mapping, click the name of the Novell NDS tree whose group set mapping you want to delete.

Result: The Group Mappings for NDS Users table appears.

Step 6 Click the group set mapping you want to delete.

Step 7 Click **Delete**.

Result: Cisco Secure ACS displays a confirmation dialog box.

Step 8 Click **OK** in the confirmation dialog box.

Result: Cisco Secure ACS deletes the selected external user database group set mapping.

Deleting a Windows NT/2000 Domain Group Mapping Configuration

You can delete an entire group mapping configuration for a Windows NT/2000 domain. When you delete a Windows domain group mapping configuration, all the group set mappings in the configuration are deleted.

To delete a Windows NT/2000 group mapping, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the name of the Windows NT/2000 external user database.

Step 4 Click the domain name whose group set mapping you want to delete.

Step 5 Click **Delete Configuration**.

Result: Cisco Secure ACS displays a confirmation dialog box.

Step 6 Click **OK** in the confirmation dialog box.

Result: Cisco Secure ACS deletes the selected external user database group mapping configuration.

Downloaded from www.Manualslib.com manuals search engine

Changing Group Set Mapping Order

You can change the order in which Cisco Secure ACS checks group set mappings for users authenticated by Windows NT/2000, Novell NDS, and generic LDAP databases. To order group mappings, you must have already mapped them. For more information about creating group mappings, see the "Creating a Cisco Secure ACS Group Mapping for Windows NT/2000, Novell NDS, or Generic LDAP Groups" section on page 12-15.

To change the order of the group mappings for a Windows NT/2000, Novell NDS, or generic LDAP group mapping, follow these steps:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the external user database name for which you want to configure group set mapping order.

Result: If you are ordering Windows NT/2000 group set mappings, the Domain Configurations table appears. If you are ordering NDS group set mappings, the NDS Trees table appears. Otherwise, the Group Mappings for *database* Users table appears.

Step 4 If you are configuring Windows NT/2000 group mapping order, click the domain name for which you want to configure group set mapping order.

Result: The Group Mappings for Domain: *domainname* table appears.

Step 5 If you are configuring Novell NDS group set mapping order, click the name of the Novell NDS tree for which you want to configure group set mapping order.

Result: The Group Mappings for NDS Users table appears.

Step 6 Click **Order mappings**.

Note The Order mappings button appears only if more than one group set mapping exists for the current database.

Result: The Order mappings for *database* page appears. The group mappings for the current database appear in the Order list.

Step 7 Select the name of a group set mapping you want to move, and then click **Up** or **Down** until it is in the position you want.

Downloaded from www.Manualslib.com manuals search engine

Step 8 Repeat Step 7 until the group mappings are in the order you need.

Step 9 Click **Submit**.

Result: The Group Mappings for *database* page displays the group set mappings in the order you defined.

RADIUS-Based Group Specification

For some types of external user databases, Cisco Secure ACS supports the assignment of users to specific Cisco Secure ACS groups based upon the RADIUS authentication response from the external user database. This is provided in addition to the unknown user group mapping described in the "Group Mapping by External User Database" section on page 12-10. RADIUS-based group specification overrides group mapping. The database types that support RADIUS-based group specification are as follows:

- LEAP Proxy RADIUS server
- CRYPTOCard token server
- ActivCard token server
- Vasco token server
- RADIUS token server

Cisco Secure ACS supports per-user group mapping for users authenticated with a LEAP Proxy RADIUS Server database. This is provided in addition to the default group mapping described in the "Group Mapping by External User Database" section on page 12-10.

Downloaded from www.Manualslib.com manuals search engine

To enable per-user group mapping, configure the external user database to return authentication responses that contain the Cisco IOS/PIX RADIUS attribute 1, [009\001] cisco-av-pair with the following value:

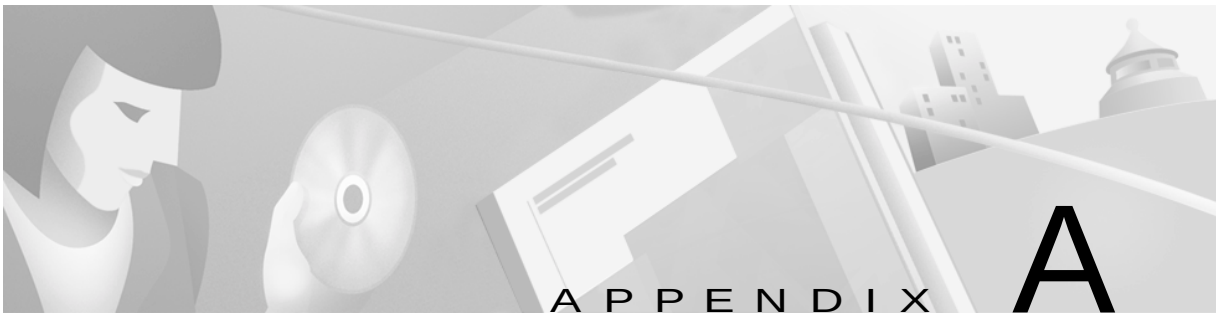
`ACS:CiscoSecure-Group-Id = N`

where *N* is the Cisco Secure ACS group number (0 through 499) to which Cisco Secure ACS should assign the user. For example, if the LEAP Proxy RADIUS Server authenticated a user and included the following value for the Cisco IOS/PIX RADIUS attribute 1, [009\001] cisco-av-pair:

`ACS:CiscoSecure-Group-Id = 37`

Cisco Secure ACS assigns the user to group 37 and applies authorization associated with group 37.

Downloaded from www.Manualslib.com manuals search engine



Troubleshooting Information for Cisco Secure ACS

This appendix provides information about some basic problems and describes how to resolve them.

Scan the column on the left to identify the condition that you are trying to resolve, and then carefully go through each corresponding recovery action offered in the column on the right.

Downloaded from www.Manualslib.com manuals search engine

Administration Issues

Condition	Recovery Action
Remote administrator cannot bring up the Cisco Secure ACS HTML interface in a browser or receives a warning that access is not permitted.	Ping the machine running Cisco Secure ACS to confirm connectivity. Verify that the remote administrator is using a valid administrator name and password that has already been added in Administration Control. Verify that Java functionality is enabled in the browser. Determine whether the remote administrator is trying to administer Cisco Secure ACS through a firewall, through a device performing network address translation, or from a browser configured to use an HTTP proxy server. For more information about accessing the HTML interface in these networking scenarios, see Network Environments and Remote Administrative Sessions, page 1-24.
Unauthorized users can log in.	Reject listed IP addresses is selected, but no start or stop IP addresses are listed. Go to Administrator Control: Access Policy and specify the Start IP Address and Stop IP Address.
Restart Services does not work.	The system is not responding. To manually restart services, from the Windows Start menu, choose **Control Panel** > **Services**. Click **CSAdmin**, and then **Stop**, and then **Start**.
Cannot install Novell NDS database authentication.	Make sure Novell Requestor is installed on the same Windows NT/2000 server as the Cisco Secure ACS.
No remote administrators can log in.	Allow only listed IP addresses to connect is selected, but no start or stop IP addresses are listed. Go to Administrator Control: Access Policy and specify the Start IP Address and Stop IP Address.
Administrator configured for event notification is not receiving e-mail.	Make sure that the SMTP server name is correct. If the name is correct, make sure that the Cisco Secure ACS machine can ping the SMTP server or can send e-mail via a third-party e-mail software package. Make sure you have not used underscores in the e-mail address.

Downloaded from www.Manualslib.com manuals search engine

Browser Issues

Condition	Recovery Action
The browser cannot bring up the Cisco Secure ACS HTML interface.	Open Internet Explorer or Netscape Navigator and choose **Help** > **About** to determine the version of the browser. See System Requirements, page 2-2 for a list of browsers supported by Cisco Secure ACS and the Release Notes for known issues with a particular browser version. For information about various network scenarios that affect remote administrative sessions, see Network Environments and Remote Administrative Sessions, page 1-24.
The browser displays the Java message that your session connection is lost.	Check the idle timeout value for remote administrators. This is in the Administration Control window. Increase the value as needed.
Administrator database appears corrupted.	The remote Netscape client is caching the password. If you specify an incorrect password, it is cached. When you attempt to reauthenticate with the correct password, the incorrect password is sent. Clear the cache before attempting to reauthenticate or close the browser and open a new session.

Downloaded from www.Manualslib.com manuals search engine

Cisco IOS Issues

Condition	Recovery Action
Under EXEC Commands, Cisco IOS commands are not being denied when checked.	Examine the Cisco IOS configuration at the AAA client. If not already present, add the following Cisco IOS command to the AAA client configuration: `aaa authorization command <0-15> default group TACACS+` The correct syntax for the arguments in the text box is **permit** *argument* or **deny** *argument*.
Administrator has been locked out of the AAA client because of an incorrect configuration being set up in the AAA client.	Try to connect directly to the AAA client at the console port. If that is not successful, consult your AAA client documentation or go to Cisco.com regarding password recovery procedures on your AAA client. For more information, see the "Cisco.com" section on page xxxiii.
IETF RADIUS attributes not supported in Cisco IOS 12.0.5.T	Cisco incorporated RADIUS (IETF) attributes in Cisco IOS Release 11.1. However, there are a few attributes that are not yet supported or that require a later version of the Cisco IOS software. The following attributes fall into this category: **Number—Attribute Supported** 17—Change Password 11.3 21—Password-Expiration 11.3 35—Login-LAT-Node No 36—Login-LAT-Group No
AAA client times out when authenticating against Windows NT/2000.	Increase the TACACS+ timeout interval from the default, 5, to 20. Set the Cisco IOS command as follows: `tacacs-server timeout 20`

Downloaded from www.Manualslib.com manuals search engine

Database Issues

Condition	Recovery Action
RDBMS Synchronization is not operating properly.	Make sure the correct server is listed in the Partners list.
Database Replication not operating properly.	Make sure you have set the server correctly as either Send or Receive. On the sending server, make sure the receiving server is in the Replication list. On the receiving server, make sure the sending server is selected in the Accept Replication from list. Make sure that the replication schedule on the sending Cisco Secure ACS is not conflicting with the replication schedule on the receiving Cisco Secure ACS. If the receiving server has dual network cards, on the sending server add a AAA server to the AAA Servers table in Network Configuration for every IP address of the receiving server. If the sending server has dual network cards, on the receiving server add a AAA server to the AAA Servers table in Network Configuration for every IP address of the receiving server.
The external user database is not available in the Group Mapping section.	The external database has not been configured in External User Databases or the username and password have been typed incorrectly. Make sure the username and password are correct. Click the applicable external database to configure.
External databases not operating properly.	Make sure a two-way trust (for dial-in check) has been established between the Cisco Secure ACS domain and the other domains. Turn logging to the maximum and check the csauth service log file for any debug messages beginning with `[External DB]`. See Setting Up Event Logging, page 8-51.

Downloaded from www.Manualslib.com manuals search engine

Dial-in Connection Issues

Condition	Recovery Action

A dial-in user is unable to make a connection to the AAA client.
 	
No record of the attempt appears in either the TACACS+ or RADIUS Accounting Report (in the **Reports & Activity** section, click **TACACS+ Accounting** or **RADIUS Accounting** or **Failed Attempts**).
	Examine the Cisco Secure ACS Reports or AAA client Debug output to narrow the problem to a system error or a user error. Confirm the following:
	• The dial-in user was able to establish a connection and ping the Windows NT/2000 server *before* Cisco Secure ACS was installed. If the dial-in user could not, the problem is related to a AAA client/modem configuration, not Cisco Secure ACS.
	• LAN connections for both the AAA client and the Windows NT/2000 server supporting Cisco Secure ACS are physically connected.
	• IP address of the AAA client in the Cisco Secure ACS configuration is correct.
	• IP address of Cisco Secure ACS in AAA client configuration is correct.
	• TACACS+ or RADIUS key in both AAA client and Cisco Secure ACS are identical (case sensitive).
	• The command **ppp authentication pap** is entered for each interface, if the Windows NT/2000 user database is being used.
	• The command **ppp authentication chap pap** is entered for each interface, if the Cisco Secure ACS database is being used.
	• The AAA and TACACS+ or RADIUS commands are correct in the AAA client. The necessary commands are listed in the following:
	`Program Files\CiscoSecure ACS v`*x.x*`\TacConfig.txt`
	`Program Files\CiscoSecure ACS v`*x.x*`\RadConfig.txt.`
	• The Cisco Secure ACS Services are running (CSAdmin, CSAuth, CSDBSync CSLog, CSRadius, CSTacacs) on the Windows NT/2000 server.

Downloaded from www.Manualslib.com manuals search engine

Condition	Recovery Action
A dial-in user is unable to make a connection to the AAA client. The Windows NT/2000 user database is being used for authentication. A record of a failed attempt appears in the Failed Attempts Report (in the **Reports & Activity** section, click **Failed Attempts**).	The user information is not properly configured for authentication in Windows NT/2000 or Cisco Secure ACS. The Windows NT/2000 user database resides on the same machine as Cisco Secure ACS. From the Windows NT User Manager or Windows 2000 Active Directory Users and Computers, confirm the following: • The username and password are configured in Windows NT User Manager or the Windows 2000 Active Directory Users and Computers. • The User Properties window does not have User Must Change Password at Login enabled. • The User Properties window does not have Account Disabled selected. • The User Properties for the dial-in window does not have Grant dial-in permission to user disabled, if Cisco Secure ACS is using this option for authenticating. From within the Cisco Secure ACS confirm the following: • If the username has already been entered into Cisco Secure ACS, a Windows NT/2000 database configuration is selected in the Password Authentication list in User Setup for the user. • If the username has already been entered into Cisco Secure ACS, the Cisco Secure ACS group to which the user is assigned has the correct authorization enabled (such as IP/PPP, IPX/PPP or Exec/Telnet). Be sure to click Submit + Restart if a change has been made. • The user's expiration information in the Windows NT/2000 database has not caused failed authentication. For troubleshooting purposes, disable password expiry for the user in the Windows NT/2000 database.

Downloaded from www.Manualslib.com manuals search engine

Condition	Recovery Action
(continued)	Click **External User Databases**, and click **List All Databases Configured**, and then make sure that the database configuration for Windows NT/2000 is listed. Check the Unknown User Policy to make sure that Fail the Attempt is not selected. Select the **Selected Databases** check box in the Unknown User Policy page in the External User Databases section. Verify that the Windows NT/2000 group that the user belongs to has not been mapped to No Access.
A dial-in user is unable to make a connection to the AAA client. The CiscoSecure user database being used for authentication. A record of a failed attempt is displayed in the Failed Attempts Report (in the **Reports & Activity** section, click **Failed Attempts**).	From within Cisco Secure ACS confirm the following: • The username has been entered into Cisco Secure ACS. • CiscoSecure user database is selected on the Password Authentication list and a password has been entered in User Setup for the user • The Cisco Secure ACS group to which the user is assigned has the correct authorization enabled (such as IP/PPP, IPX/PPP or Exec/Telnet). Be sure to click Submit + Restart if a change has been made. • Expiration information has not caused failed authentication. Set to Expiration: Never for troubleshooting.

Downloaded from www.Manualslib.com manuals search engine

Condition	Recovery Action

A dial-in user is unable to make a connection to the AAA client; however, a Telnet connection can be authenticated across the LAN.	This isolates the problem to one of three areas:
	• Line/modem configuration problem. Review the documentation that came with your modem and verify that the modem is properly configured.
	• The user is not assigned to a group that has the correct authorization rights. Authorization rights can be modified under Group Setup or User Setup. User settings override group settings.
	• The Cisco Secure ACS or TACACS+ or RADIUS configuration is not correct in the AAA client. The necessary commands are listed in the following:
	`Program Files\CiscoSecure ACS v`*x.x*`\TacConfig.txt`
	`Program Files\CiscoSecure ACS v`*x.x*`\RadConfig.txt`
	`Program Files\CiscoSecure ACS v`*x.x*`\README.TXT`
	You can additionally verify Cisco Secure ACS connectivity as follows:
	• Telnet to the access server from a workstation connected to the LAN.
	A successful authentication for Telnet confirms that Cisco Secure ACS is working with the AAA client.

Downloaded from www.Manualslib.com manuals search engine

Condition	Recovery Action

A dial-in user is unable to make a connection to the AAA client, and a Telnet connection cannot be authenticated across the LAN.	Determine if the Cisco Secure ACS is receiving the request. This can be done by viewing the Cisco Secure ACS reports. Based on what does not appear in the reports and which database is being used, troubleshoot the problem based on one of the following:
	• Line/modem configuration problem. Review the documentation that came with your modem and verify that the modem is properly configured.
	• The user does not exist in the Windows NT/2000 user database or the CiscoSecure user database and might not have the correct password. Authentication parameters can be modified under User Setup.
	• The Cisco Secure ACS or TACACS+ or RADIUS configuration is not correct in the AAA client. The necessary commands are listed in the following:
	`Program Files\CiscoSecure ACS v`*`x.x`*`\TacConfig.txt`
	`Program Files\CiscoSecure ACS v`*`x.x`*`\RadConfig.txt`
	`Program Files\CiscoSecure ACS v`*`x.x`*`\README.TXT`

Downloaded from www.Manualslib.com manuals search engine

Debug Issues

Condition	Recovery Action

When running **debug aaa authentication** on the AAA client, a failure message is returned from Cisco Secure ACS.	The configurations of the AAA client or Cisco Secure ACS are likely to be at fault.
	
	From within Cisco Secure ACS confirm the following:
	
	• Cisco Secure ACS is receiving the request. This can be done by viewing the Cisco Secure ACS reports. Based on what does/does not appear in the reports and which database is being used, troubleshoot Cisco Secure ACS based on one of the first three listings in this matrix.
	
	From the AAA client, confirm the following:
	
	• The command **ppp authentication pap** is entered for each interface if authentication against the Windows NT/2000 User Database is being used.
	
	• The command **ppp authentication chap pap** is entered for each interface if authentication against the CiscoSecure user database is being used.
	
	• The AAA and TACACS+ or RADIUS configuration is correct in the AAA client. The necessary commands are listed in the following:
	
	`Program Files\CiscoSecure ACS v`*x.x*`\TacConfig.txt`
	`Program Files\CiscoSecure ACS v`*x.x*`\RadConfig.txt`
	`Program Files\CiscoSecure ACS v`*x.x*`\README.TXT`

When running **debug aaa authentication** and **debug aaa authorization** on the AAA client, a `PASS` is returned for authentication, but a `FAIL` is returned for authorization.	This problem occurs because authorization rights are not correctly assigned. From Cisco Secure ACS User Setup, confirm that the user is assigned to a group that has the correct authorization rights. Authorization rights can be modified under Group Setup or User Setup. User settings override group settings. If a specific attribute for TACACS+ or RADIUS is not displayed within the Group Setup section, this might indicate it has not been enabled in Interface Configuration: TACACS+ (Cisco IOS) or RADIUS.

Downloaded from www.Manualslib.com manuals search engine

Proxy Issues

Condition	Recovery Action
Proxy fails.	Make sure that the direction on the remote server is set to Incoming/Outgoing or Incoming, and that the direction on the authentication forwarding server is set to Incoming/Outgoing or Outgoing. Make sure the shared secret (key) matches the shared secret of one or both Cisco Secure ACS servers. Make sure the character string and delimiter match the stripping information configured in the Proxy Distribution Table, and the position is set correctly to either Prefix or Suffix. One or more servers is down, or no fallback server is configured. Go to Network Configuration and configure a fallback server. Fallback servers are used only under the following circumstances: • The remote Cisco Secure ACS is down. • One or more services (CSTacacs, CSRadius, or CSAuth) are down. • The secret key is misconfigured. • Inbound/Outbound messaging is misconfigured.

Downloaded from www.Manualslib.com manuals search engine

Installation and Upgrade Issues

Condition	Recovery Action
The following error message displays when you try to upgrade or uninstall Cisco Secure ACS: `The following file is invalid or the data is corrupted "DelsL1.isu"`	From the Windows NT/2000 Registry, delete the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CiscoSecure`
All previous accounting logs are missing.	If you are reinstalling or upgrading the Cisco Secure ACS software, the files are deleted unless moved to another directory location.

MaxSessions Issues

Condition	Recovery Action
MaxSessions over VPDN is not working.	The use of MaxSessions over VPDN is not supported.
User MaxSessions fluctuates or is unreliable.	Services were restarted, possibly because the connection between the Cisco Secure ACS and the AAA client is unstable. Clear the **Single Connect TACACS+ AAA Client** check box.

Downloaded from www.Manualslib.com manuals search engine

Report Issues

Condition	Recovery Action
The `active.csv` report is blank.	You changed protocol configurations recently. Whenever protocol configurations change, the existing `active.csv` report file is renamed to *yyyy-mm-dd*`.csv`, and a new, blank `active.csv` report is generated
A report is blank.	Make sure you have selected Log to *reportname* Report under System Configuration: Logging: Log Target: *reportname*. You must also set Network Configuration: *servername*: Access Server Type to CiscoSecure ACS for Windows NT.
No Unknown User information is included in reports.	The Unknown User database was changed. Accounting reports will still contain unknown user information.
Two entries are logged for one user session.	Make sure that remote logging and the Send Accounting Information fields in the Proxy Distribution Table are not configured to send accounting packets to the same location.
After you have changed the date format, the Logged-In User list and CSAdmin log still display old format dates.	Restart the csadmin services by clicking X in the upper right corner of the HTML interface.

Downloaded from www.Manualslib.com manuals search engine

Third-Party Server Issues

Condition	Recovery Action
You cannot properly implement the RSA token server.	1. Log in to the Windows NT/2000 Server on which Cisco Secure ACS is installed. (Make sure your login account has administrative privileges.) 2. Make sure the RSA Client software is installed on the same WindowsNT/2000 server as the Cisco Secure ACS. 3. Follow the setup instructions. Do not restart at the end of the installation. 4. Get the file named sdconf.rec located in the /data directory of the RSA ACE server. 5. Place sdconf.rec on the WindowsNT/2000 Server in the `%SystemRoot%\system32` directory. 6. Make sure you can ping the machine that is running the ACE server by hostname. (You might need to add the machine in the lmhosts file.) 7. Verify that support for RSA is enabled in External User Database: Database Configuration in the Cisco Secure ACS. 8. Run Test Authentication from the WindowsNT/2000 Server control panel for the ACE/Client application. 9. From Cisco Secure ACS, install the token server.

Downloaded from www.Manualslib.com manuals search engine

PIX Firewall Issues

Condition	Recovery Action
Remote administrator cannot bring up Cisco Secure ACS from his or her browser or receives a warning that access is not permitted.	If Network Address Translation is enabled on the PIX Firewall, administration through the firewall cannot work. To administer Cisco Secure ACS through a firewall, you must configure an HTTP port range in System Configuration: Access Policy. The PIX Firewall must be configured to permit HTTP traffic over all ports included in the range specified in Cisco Secure ACS. For more information, see Access Policy, page 10-10.

User Authentication Issues

Condition	Recovery Action
After the administrator removes the Check NT Callback setting from External User Databases: Database Configuration: Windows NT/2000: Configuration, Windows NT/2000 database users can still dial in and apply the Callback string configured under the Windows NT/2000 user database.	Restart the Cisco Secure ACS services.
Callback is not working.	Ensure that callback works on the AAA client using local authentication. Then add AAA authentication.
User authentication fails when using PAP.	Outbound PAP is not enabled. If the Failed Attempts report shows that you are using outbound PAP, go to Interface Configuration and select the **Per-User Advanced TACACS+ Features** check box. Then, go to User Setup: Advanced TACACS+ Settings. Click **TACACS+ Enable Control** and type and confirm the password in the TACACS+ Outbound Password box.

Downloaded from www.Manualslib.com manuals search engine

Condition	Recovery Action
Unknown users are not authenticated.	Go to External User Databases: Unknown User Policy. Click **Check the following external user databases**. From the External Databases list, select the database(s) against which to authenticate unknown users. Click —> (right arrow button) to add the database to the Selected Databases list. Click **Up** or **Down** to move the database into the desired position in the authentication hierarchy. If you are using the Cisco Secure ACS Unknown User feature, external databases can authenticate using only PAP.
User did not inherit settings from new group.	Users moved to a new group inherit new group settings but they keep their existing user settings. Manually change the settings in User Settings.
User can authenticate but authorizations are different from expected.	Different vendors use different AV pairs. AV pairs not used in one vendor's protocol are ignored by another vendor's protocol. Make sure the user settings reflect the correct vendor protocol; for example, Cisco RADIUS.
User cannot log in.	Re-enable the user account or reset the failed attempts counter.
Authentication fails.	The retry interval is too short. (The default is 5 seconds.) Increase the retry interval (**tacacs-server timeout 20**) on the AAA client to 20 or greater. Check the Failed Attempts report.

Downloaded from www.Manualslib.com manuals search engine

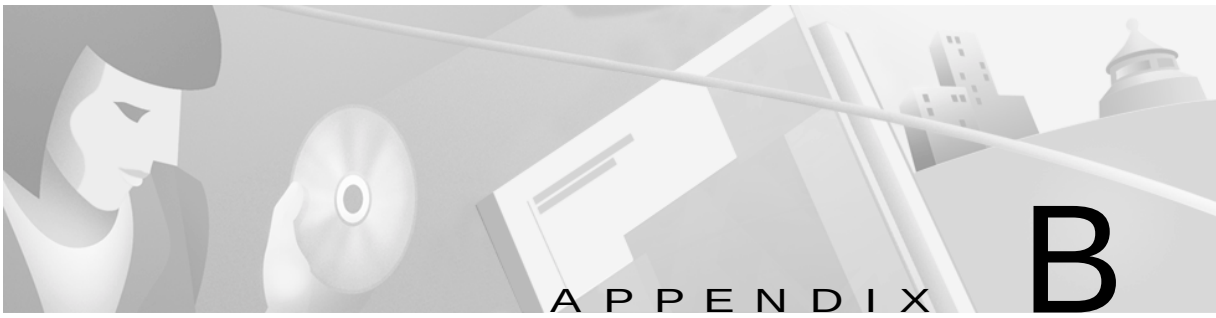
TACACS+ and RADIUS Attribute Issues

Condition	Recovery Action

TACACS+ and RADIUS attributes do not appear on the Group Setup page.	Ensure that you have at least one RADIUS or TACACS+ AAA client configured in the Network Configuration section and that, in the Interface Configuration section, you have enabled the attributes you need to configure.
	
	Note Some attributes are not customer-configurable in Cisco Secure ACS; instead, their values are set by Cisco Secure ACS.
	
	Beginning with Cisco Secure ACS Version 2.3, some TACACS+ attributes no longer appear on the Group Setup page. This is because IP pools and callback supersede the following attributes:
	
	TACACS+
	
	`addr`
	`addr-pool`
	`callback-dialstring`
	
	Ascend RADIUS
	
	`8, Framed-IP-Address`
	`19, Callback-Number`
	`218, Ascend-Assign-IP-Pool`
	
	Additionally, these attributes cannot be set via database synchronization, and `ip:addr=n.n.n.n` is not allowed as a Cisco vendor-specific attribute (VSA)

Novell NDS or Generic LDAP Group Mapping not working correctly.	Make sure you have correctly configured Group Mapping for the applicable database. For more information, see Database Group Mappings, page 12-10.

Downloaded from www.Manualslib.com manuals search engine



System Messages

This appendix contains a partial list of system messages for Cisco Secure ACS, an explanation of their meanings, and recommended action to resolve any problems.

Windows NT/2000 Event Log Service Startup Errors

Error Message `Could not initialize Crypto module`

Explanation The Microsoft Crypto API failed to initialize.

Recommended Action Make sure you are running the U.S. version of Windows NT/2000. Make sure the Crypto API files are not missing or corrupted.

Error Message `Failed to initialize working directories/files`

Explanation The Registry might be corrupt, or the files under the CSAuth folder might be missing or busy.

Recommended Action Reinstall Cisco Secure ACS

Downloaded from www.Manualslib.com manuals search engine

Error Message One or more registry entries were missing/corrupt

Explanation The CSAuth Registry either is corrupt or has missing values.

Recommended Action Reinstall Cisco Secure ACS.

System Monitored Events

Error Message Auth server down: Could not change Password

Explanation CSMon could not change the password of the test account.

Recommended Action No action required.

Error Message CSMon obtained an authentication via a CiscoSecure service.

Recommended Action No action required.

Error Message **Error Message** *name*: Failed to authenticate on test account

Explanation CSMon failed to get an authentication via a CiscoSecure service.

Recommended Action No action required.

Error Message *name*: Failed to logon to test account.

Explanation CSMon failed to log in via a CiscoSecure service.

Recommended Action No action required.

Error Message *name*: Failed to logoff from test account

Explanation CSMon failed to log off via a CiscoSecure service.

Recommended Action No action required.

Downloaded from www.Manualslib.com manuals search engine

Error Message *name*: Logged Off

Explanation CSMon logged off via a CiscoSecure service.

Recommended Action No action required

Error Message *name*: Logged On

Explanation CSMon obtained a login via a CiscoSecure service.

Recommended Action No action required.

Error Message Monitoring of *name* stopped as a service *name* was stopped properly

Explanation A CiscoSecure service was shut down because a service it depended on has been shut down.

Recommended Action No action required.

Error Message Problem Authenticating from *name*. Got as far as *phase*

Explanation CSMon could not authenticate a test account via a CiscoSecure service. *phase* is one of the following:

- Launching Request to Protocol Module
- Starting Processing in Protocol Module
- Finishing Processing Protocol Module
- Starting Processing in Auth Module
- Finishing Processing in Auth Module
- Logging

Recommended Action No action required.

Downloaded from www.Manualslib.com manuals search engine

Error Message Problem Logging on to *name*. Got as far as *phase*

Explanation CSMon could not log on to the named account via a CiscoSecure service. *phase* is one of the following:

- Launching Request to Protocol Module
- Starting Processing in Protocol Module
- Finishing Processing Protocol Module
- Starting Processing in Auth Module
- Finishing Processing in Auth Module
- Logging

Recommended Action No action required.

Error Message Problem Logging Off from *name*. Got as far as *phase*

Explanation CSMon could not log off from the named account via a CiscoSecure service. *phase* is one of the following:

- Launching Request to Protocol Module
- Starting Processing in Protocol Module
- Finishing Processing Protocol Module
- Starting Processing in Auth Module
- Finishing Processing in Auth Module
- Logging

Recommended Action No action required.

Error Message Problem Logging on to *name*. Got as far as *phase*

Explanation CSMon could not log on to the named account via a CiscoSecure service. *phase* is one of the following:

- Launching Request to Protocol Module
- Starting Processing in Protocol Module
- Finishing Processing Protocol Module

Downloaded from www.Manualslib.com manuals search engine

- Starting Processing in Auth Module
- Finishing Processing in Auth Module
- Logging

Recommended Action No action required

Error Message Service *name* could not be restarted

Explanation CSMon has failed to restart the named CiscoSecure service.

Recommended Action Manually start the applicable service from the command line or choose **Start** > **Settings** > **Control Panel** and then click **Services** and use the Services applet to start the applicable service

Error Message Service *name* has been restarted so monitoring will now continue

Explanation The named CiscoSecure service has been restarted via the Windows NT/2000 Service Manager.

Recommended Action No action required.

Error Message Service *name* has been stopped properly. Monitoring will suspend until the service is restarted

Explanation The named CiscoSecure service was shut down via the Windows NT/2000 Service Manager

Recommended Action No action required.

Error Message Service *name* in transition state for too long... giving up

Explanation CSMon waits only so long before giving up on a transitory service.

Recommended Action No action required

Downloaded from www.Manualslib.com manuals search engine

Error Message Service *name* in transition/unknown state... will try again

Explanation Windows NT/2000 Service Manager does not know what state a service is in.

Recommended Action No action required.

Error Message Service *name* not running: will attempt to restart

Explanation CSMon has detected that the named CiscoSecure service is not running.

Recommended Action No action required

Error Message Service *name* re-started OK

Explanation CSMon has restarted the named CiscoSecure service

Recommended Action No action required.

Replication Messages

Error Message Cannot replicate to '*name*'- server not responding

Explanation The named destination Cisco Secure ACS system was unreachable

Recommended Action Check the connectivity between the remote Cisco Secure ACS and the replicating ACS. Verify that the IP address of the AAA server is correct under AAA entry.

Downloaded from www.Manualslib.com manuals search engine

Error Message Database synchronization with host *name* failed - refer to CSAuth log file

Explanation Part of the configuration set could not be sent to the named Cisco Secure ACS.

Recommended Action Check the CSAuth log file to view the cause of the failure. The CSAuth log file is located in `Program Files\Cisco Secure ACS v2.6\CSAuth\logs`.

Error Message Failed to send one or more files to host 'n*ame*'

Explanation Part of the replication set was not successfully sent to the remote Cisco Secure ACS.

Recommended Action Check the connectivity between the remote Cisco Secure ACS and the replicating ACS. Verify that the IP address of the AAA server is correct under AAA entry.

Error Message Host '*name' has* denied replication request

Explanation Remote Cisco Secure ACS did not authorize replication.

Recommended Action Verify that the remote ACS is accepting replication in System Configuration: CiscoSecure Database Replication.

Error Message Host '*name' not* replied to replication request - possibly dead

Explanation Remote Cisco Secure ACS did not respond to replication commit command.

Recommended Action Check the systems' connectivity.

Downloaded from www.Manualslib.com manuals search engine

Error Message Host ‘n*ame’ not* configured to receive any matching information

Explanation The remote Cisco Secure ACS is not configured to accept the information offered.

Recommended Action Verify that the remote ACS has at least some replication components checked.

Error Message Inbound database replication from host ‘n*ame*’ denied

Explanation Remote Cisco Secure ACS not authorized to replicate to this Cisco Secure ACS.

Recommended Action Configure the remote Cisco Secure ACS to replicate to this Cisco Secure ACS.

Error Message Inbound database replication from remote host has errors - refer to CSAuth logfile

Explanation Inbound replication failed or was only partially successful.

Recommended Action Check the CSAuth log file to view the cause of the error. The CSAuth log file is located in:
`Program Files\Cisco Secure ACS v`*`x.x`*`\CSAuth\logs`.

Error Message Initiating outbound database replication

Explanation CSAuth has started to replicate configuration information to another Cisco Secure ACS.

Recommended Action No action required.

Error Message Outbound database replication completed

Explanation CSAuth has completed replication.

Recommended Action No action required.

Downloaded from www.Manualslib.com manuals search engine

Error Message Outbound database replication failed - refer to CSAuth log file

Explanation Replication failed or was only partially successful.

Recommended Action Check the CSAuth log file to view the cause of the failure. The CSAuth log file is located in:
`Program Files\Cisco Secure ACS v`*`x.x`*`\CSAuth\logs`.

Failed Attempts Messages

Error Message Auth type not supported by External DB

Explanation External DLL is not configured for requested authentication type.

Recommended Action No action is required.

Error Message Cached token rejected/expired

Explanation The cached token is incorrect or has expired.

Recommended Action Enter or re-enter the correct token.

Error Message Failed to Allocate IP Address For User

Explanation Internal error.

Recommended Action The ACS pool has run out of available IP addresses. Extend the IP address ranges.

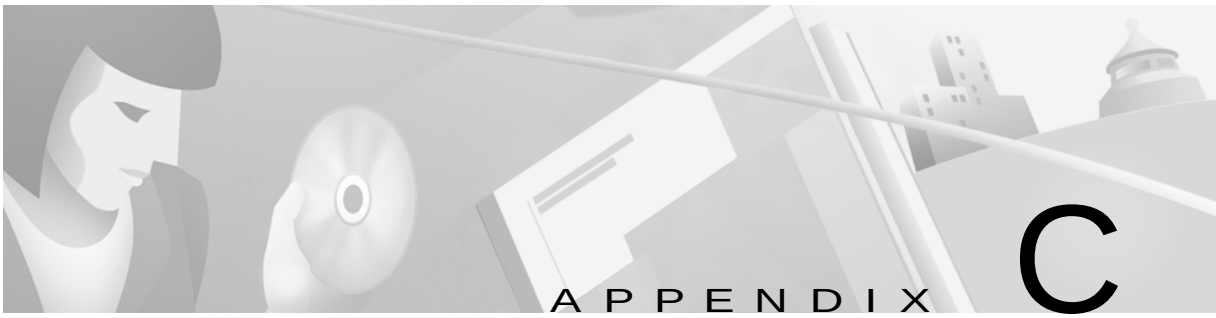
Error Message Key Mismatch

Explanation The AAA client secret key did not match the Cisco Secure ACS configured key.

Recommended Action Check the shared key between the Cisco Secure ACS and the AAA server.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine



TACACS+ Attribute-Value Pairs

Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) provides support for Terminal Access Controller Access Control System (TACACS+) attribute-value (AV) pairs. You can enable different AV pairs for any supported attribute value.

Cisco IOS Attribute-Value Pair Dictionary

Before selecting TACACS+ AV pairs for Cisco Secure ACS, confirm that your AAA client is running Cisco IOS Release 11.2 or later. Earlier versions of Cisco IOS work with Cisco Secure ACS but do not fully support the TACACS+ features in Cisco Secure ACS.

Note If you specify a given AV pair in Cisco Secure ACS, you must also enable the corresponding AV pair in the Cisco IOS software running on the AAA client. Therefore, you must consider which AV pairs your Cisco IOS release supports. If Cisco Secure ACS sends an AV pair to the AAA client that the Cisco IOS software does not support, that attribute is not implemented.

For more information on TACACS+ AV pairs, refer to Cisco IOS documentation for the release of Cisco IOS running on your AAA clients.

Note All TACACS+ values are strings. The concept of value “type” does not exist in TACACS+ as it does in Remote Access Dial-In User Service (RADIUS).

Downloaded from www.Manualslib.com manuals search engine

TACACS+ AV Pairs

Note Beginning with Cisco Secure ACS 2.3, some TACACS+ attributes no longer appear on the Group Setup page. This is because IP pools and callback supersede the following attributes:

addr
addr-pool
callback-dialstring

Additionally, these attributes cannot be set via database synchronization, and **ip:addr=n.n.n.n** is not allowed as a Cisco vendor-specific attribute (VSA).

Cisco Secure ACS supports many TACACS+ AV pairs. For descriptions of these attributes, refer to Cisco IOS documentation for the release of Cisco IOS running on your AAA clients. TACACS+ AV Pairs supported in Cisco Secure ACS are as follows:

- acl=
- addr=
- addr-pool=
- autocmd=
- callback-dialstring
- callback-line
- callback-rotary
- cmd-arg=
- cmd=
- dns-servers=
- gw-password
- idletime=
- inacl#*n*
- inacl=
- interface-config=

Downloaded from www.Manualslib.com manuals search engine

- ip-addresses
- link-compression=
- load-threshold=*n*
- max-links=*n*
- nas-password
- nocallback-verify
- noescape=
- nohangup=
- old-prompts
- outacl#*n*
- outacl=
- pool-def#*n*
- pool-timeout=
- ppp-vj-slot-compression
- priv-lvl=
- protocol=
- route
- route#*n*
- routing=
- rte-ftr-in#*n*
- rte-ftr-out#*n*
- sap#*n*
- sap-fltr-in#*n*
- sap-fltr-out#*n*
- service=
- source-ip=

Downloaded from www.Manualslib.com manuals search engine

- timeout=
- tunnel-id
- wins-servers=
- zonelist=

TACACS+ Accounting AV Pairs

Cisco Secure ACS supports many TACACS+ accounting AV pairs. For descriptions of these attributes, see Cisco IOS documentation for the release of Cisco IOS running on your AAA clients. TACACS+ accounting AV pairs supported in Cisco Secure ACS are as follows:

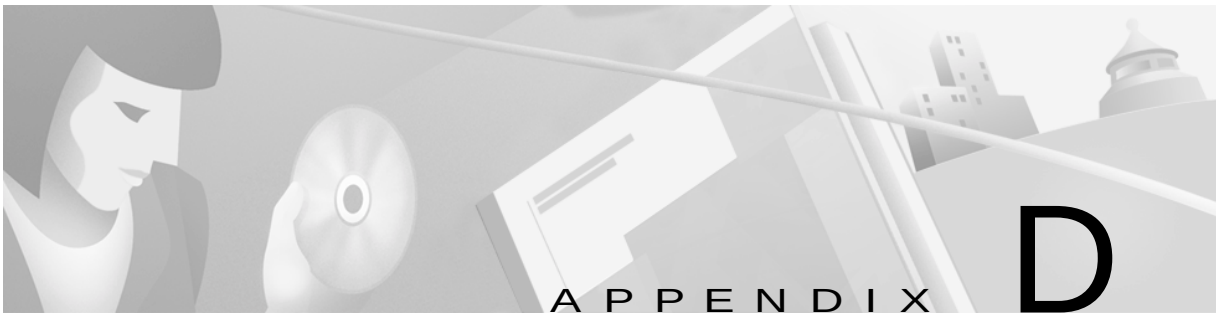
- bytes_in
- bytes_out
- cmd
- data-rate
- disc-cause
- disc-cause-ext
- elapsed_time
- event
- mlp-links-max
- mlp-sess-id
- nas-rx-speed
- nas-tx-speed
- paks_in
- paks_out
- port
- pre-bytes-in
- pre-bytes-out
- pre-paks-in
- pre-paks-out

Downloaded from www.Manualslib.com manuals search engine

- pre-session-time
- priv_level
- protocol
- reason
- service
- start_time
- stop_time
- task_id
- timezone
- xmit-rate

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine



RADIUS Attributes

Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) provides support for many RADIUS attributes. This appendix lists the standard attributes, vendor-proprietary attributes, vendor-specific attributes supported by Cisco Secure ACS for the following vendors' implementations of RADIUS:

- Cisco IOS RADIUS
- Cisco VPN 3000 Concentrator RADIUS
- Cisco VPN 5000 Concentrator RADIUS
- Cisco Building Broadband Service Manager RADIUS
- Microsoft RADIUS
- Ascend RADIUS
- Nortel RADIUS
- Juniper RADIUS
- Internet Engineering Task Force (IETF) RADIUS

You can enable different AV pairs for any supported vendors. The supported RADIUS AV pairs specific to each vendor are listed in this appendix:

- Cisco IOS Dictionary of RADIUS AV Pairs, page D-2
- Cisco IOS/PIX Dictionary of RADIUS VSAs, page D-4
- Cisco VPN 3000 Concentrator Dictionary of RADIUS VSAs, page D-6
- Cisco VPN 5000 Concentrator Dictionary of RADIUS VSAs, page D-9

Downloaded from www.Manualslib.com manuals search engine

- Cisco Building Broadband Service Manager Dictionary of RADIUS VSA, page D-9
- Vendor-Proprietary IETF RADIUS AV Pairs, page D-10
- IETF Dictionary of RADIUS AV Pairs, page D-12
- Microsoft MPPE Dictionary of RADIUS VSAs, page D-18
- Ascend Dictionary of RADIUS AV Pairs, page D-21
- Nortel Dictionary of RADIUS VSAs, page D-29
- Juniper Dictionary of RADIUS VSAs, page D-30

Cisco IOS Dictionary of RADIUS AV Pairs

Cisco Secure ACS supports Cisco IOS RADIUS attribute-value (AV) pairs. Before selecting AV pairs for Cisco Secure ACS, confirm that your AAA client is a compatible release of Cisco IOS or compatible AAA client software. For more information, see the "System Requirements" section on page 2-2.

Note If you specify a given AV pair on Cisco Secure ACS, the corresponding AV pair must be implemented in the Cisco IOS software running on the network device. Always take into consideration which AV pairs your Cisco IOS release supports. If Cisco Secure ACS sends an AV pair that the Cisco IOS software does not support, the attribute is not implemented.

Note Beginning with Cisco Secure ACS version 2.3, some RADIUS attributes do not appear on the Group Setup page. This is because IP pools and callback supersede the following attributes:

8, Framed-IP-Address
19, Callback-Number
218, Ascend-Assign-IP-Pool

Neither can these attributes be set via RDBMS Synchronization.

Downloaded from www.Manualslib.com manuals search engine

Table D-1 lists the supported Cisco IOS RADIUS AV pairs.

Table D-1 Cisco IOS Software RADIUS AV Pairs

Attribute	Number	Type of Value
User-Name	1	string
User-Password	2	string
CHAP-Password	3	string
NAS-IP Address	4	ipaddr
NAS-Port	5	integer
Service-Type	6	integer
Framed-Protocol	7	integer
Framed-IP-Netmask	9	ipaddr
Framed-Routing	10	integer
Filter-Id	11	string
Framed-MTU	12	integer
Framed-Compression	13	integer
Login-IP-Host	14	ipaddr
Login-Service	15	integer
Login-TCP-Port	16	integer
Old-Password	17	string
Reply-Message	18	string
Expiration	21	date
Framed-Route	22	string
State	24	string
Class	25	string
Vendor specific	26	string
Session-Timeout	27	integer
Idle-Timeout	28	integer
Called-Station-ID	30	string

Downloaded from www.Manualslib.com manuals search engine

Table D-1 Cisco IOS Software RADIUS AV Pairs (continued)

Attribute	Number	Type of Value
Calling-Station-ID	31	string
Login-LAT-Service	33	string
Acct-Status-Type	40	integer
Acct-Delay-Time	41	integer
Acct-Input-Octets	42	integer
Acct-Output-Octets	43	integer
Acct-Session-ID	44	string
Acct-Authentic	45	integer
Acct-Session-Time	46	integer
Acct-Input-Packets	47	integer
Acct-Output-Packets	48	integer
Acct-Terminate-Cause	49	integer
NAS-Port-Type	61	integer
NAS-Port-Limit	62	integer

Cisco IOS/PIX Dictionary of RADIUS VSAs

Cisco Secure ACS supports Cisco IOS/PIX vendor-specific attributes (VSAs). The vendor ID for this Cisco RADIUS Implementation is 009. Table D-2 on page D-5 lists the supported Cisco IOS/PIX RADIUS VSAs.

Note For a discussion of Cisco IOS/PIX RADIUS VSA 1, cisco-av-pair, see AV pair 26 in Table D-7 on page D-12.

Note For details about the Cisco IOS H.323 VSAs, refer to Cisco IOS Voice-over-IP documentation.

Downloaded from www.Manualslib.com manuals search engine

Note For details about the Cisco IOS Node Route Processor-Service Selection Gateway VSAs (VSAs 250, 251, and 252), refer to Cisco IOS documentation.

Table D-2 Cisco IOS/PIX RADIUS VSAs

Attribute	Number	Type of Value
cisco-av-pair	1	string
cisco-vsa-port-string	2	string
cisco-h323-remote-address	23	string
cisco-h323-conf-id	24	string
cisco-h323-setup-time	25	string
cisco-h323-call-origin	26	string
cisco-h323-call-type	27	string
cisco-h323-connect-time	28	string
cisco-h323-disconnect-time	29	string
cisco-h323-disconnect-cause	30	string
cisco-h323-voice-quality	31	string
cisco-h323-gw-id	33	string
cisco-h323-incoming-conn-id	35	string
cisco-h323-credit-amount	101	string
cisco-h323-credit-time	102	string
cisco-h323-return-code	103	string
cisco-h323-prompt-id	104	string
cisco-h323-day-and-time	105	string
cisco-h323-redirect-number	106	string
cisco-h323-preferred-lang	107	string
cisco-h323-redirect-ip-addr	108	string
cisco-h323-billing-model	109	string
cisco-h323-currency	110	string

Downloaded from www.Manualslib.com manuals search engine

Table D-2 Cisco IOS/PIX RADIUS VSAs (continued)

Attribute	Number	Type of Value
cisco-ssg-account-info	250	string
cisco-ssg-service-info	251	string
cisco-ssg-control-info	253	string

Cisco VPN 3000 Concentrator Dictionary of RADIUS VSAs

Cisco Secure ACS supports Cisco VPN 3000 RADIUS VSAs. The vendor ID for this Cisco RADIUS Implementation is 3076. Table D-3 lists the supported Cisco VPN 3000 Concentrator RADIUS VSAs.

Note Some of the RADIUS VSAs supported by Cisco VPN 3000 Concentrators are interdependent. Before you implement them, we recommend that you refer to Cisco VPN 3000-series Concentrator documentation.

Table D-3 Cisco VPN 3000 Concentrator RADIUS VSAs

Attribute	Number	Type of Value
CVPN3000-Access-Hours	1	string
CVPN3000-Simultaneous-Logins	2	integer
CVPN3000-Primary-DNS	5	ipaddr
CVPN3000-Secondary-DNS	6	ipaddr
CVPN3000-Primary-WINS	7	ipaddr
CVPN3000-Secondary-WINS	8	ipaddr
CVPN3000-SEP-Card-Assignment	9	integer
CVPN3000-Tunneling-Protocols	11	integer
CVPN3000-IPSec-Sec-Association	12	string

Downloaded from www.Manualslib.com manuals search engine

Table D-3 Cisco VPN 3000 Concentrator RADIUS VSAs (continued)

Attribute	Number	Type of Value
CVPN3000-IPSec-Authentication	13	integer
CVPN3000-IPSec-Banner1	15	string
CVPN3000-IPSec-Allow-Passwd-Store	16	integer
CVPN3000-Use-Client-Address	17	integer
CVPN3000-PPTP-Encryption	20	integer
CVPN3000-L2TP-Encryption	21	integer
CVPN3000-IPSec-Split-Tunnel-List	27	string
CVPN3000-IPSec-Default-Domain	28	string
CVPN3000-IPSec-Tunnel-Type	30	integer
CVPN3000-IPSec-Mode-Config	31	integer
CVPN3000-IPSec-User-Group-Lock	33	integer
CVPN3000-IPSec-Over-UDP	34	integer
CVPN3000-IPSec-Over-UDP-Port	35	integer
CVPN3000-IPSec-Banner2	36	string
CVPN3000-PPTP-MPPC-Compression	37	integer
CVPN3000-L2TP-MPPC-Compression	38	integer
CVPN3000-IPSec-IP-Compression	39	integer
CVPN3000-IPSec-IKE-Peer-ID-Check	40	integer
CVPN3000-IKE-Keep-Alives	41	integer
CVPN3000-IPSec-Auth-On-Rekey	42	integer
CVPN3000-Required-Client-Firewall-Vendor-Code	45	integer
CVPN3000-Required-Client-Firewall-Product-Code	46	integer
CVPN3000-Required-Client-Firewall-Description	47	string
CVPN3000-Require-HW-Client-Auth	48	integer
CVPN3000-Require-Individual-User-Auth	49	integer
CVPN3000-Authenticated-User-Idle-Timeout	50	integer

Downloaded from www.Manualslib.com manuals search engine

Table D-3 Cisco VPN 3000 Concentrator RADIUS VSAs (continued)

Attribute	Number	Type of Value
CVPN3000-Cisco-IP-Phone-Bypass	51	integer
CVPN3000-User-Auth-Server-Name	52	string
CVPN3000-User-Auth-Server-Port	53	integer
CVPN3000-User-Auth-Server-Secret	54	string
CVPN3000-IPSec-Split-Tunneling-Policy	55	integer
CVPN3000-IPSec-Required-Client-Firewall-Capability	56	integer
CVPN3000-IPSec-Client-Firewall-Filter-Name	57	string
CVPN3000-IPSec-Client-Firewall-Filter-Optional	58	integer
CVPN3000-IPSec-Backup-Servers	59	integer
CVPN3000-IPSec-Backup-Server-List	60	string
CVPN3000-Strip-Realm	135	integer

Downloaded from www.Manualslib.com manuals search engine

Cisco VPN 5000 Concentrator Dictionary of RADIUS VSAs

Cisco Secure ACS supports the Cisco VPN 5000 RADIUS VSAs. The vendor ID for this Cisco RADIUS Implementation is 255. Table D-4 lists the supported Cisco VPN 5000 Concentrator RADIUS VSAs.

Table D-4 Cisco VPN 5000 Concentrator RADIUS VSAs

Attribute	Number	Type of Value
CVPN5000-Tunnel-Throughput	001	integer
CVPN5000-Client-Assigned-IP	002	string
CVPN5000-Client-Real-IP	003	string
CVPN5000-VPN-GroupInfo	004	string
CVPN5000-VPN-Password	005	string
CVPN5000-Echo	006	integer
CVPN5000-Client-Assigned-IPX	007	integer

Cisco Building Broadband Service Manager Dictionary of RADIUS VSA

Cisco Secure ACS supports a Cisco Building Broadband Service Manager (BBSM) RADIUS VSA. The vendor ID for this Cisco RADIUS Implementation is 5263. Table D-5 lists the supported Cisco BBSM RADIUS VSA.

Table D-5 Cisco BBSM RADIUS VSA

Attribute	Number	Type of Value
CBBSM-Bandwidth	001	integer

Downloaded from www.Manualslib.com manuals search engine

Vendor-Proprietary IETF RADIUS AV Pairs

Table D-6 lists the supported vendor-proprietary RADIUS (IETF) attributes

Table D-6 Vendor-Proprietary RADIUS Attributes

No.	Vendor-Proprietary Attribute
17	Change-Password
21	Password-Expiration
135	Primary-DNS-Server
136	Secondary-DNS-Server
187	Multilink-ID
188	Num-In-Multilink
190	Pre-Input-Octets
191	Pre-Output-Octets
192	Pre-Input-Packets
193	Pre-Output-Packets
194	Maximum-Time
195	Disconnect-Cause
197	Data-Rate
198	PreSession-Time
208	PW-Lifetime
209	IP-Direct
210	PPP-VJ-Slot-Comp
218	Assign-IP-pool
228	Route-IP
233	Link-Compression
234	Target-Utils
235	Maximum-Channels
242	Data-Filter

Downloaded from www.Manualslib.com manuals search engine

Table D-6 Vendor-Proprietary RADIUS Attributes (continued)

No.	Vendor-Proprietary Attribute
243	Call-Filter
244	Idle-Limit

Downloaded from www.Manualslib.com manuals search engine

IETF Dictionary of RADIUS AV Pairs

Table D-7 lists the supported RADIUS (IETF) attributes. If the attribute has a security server-specific format, the format is specified. Accounting attributes are listed in Table D-8 on page D-16.

Table D-7 RADIUS (IETF) Attributes

No.	Attribute	Description
1	User-Name	Name of the user being authenticated.
2	User-Password	User's password or input following an access challenge. Passwords longer than 16 characters are encrypted using IETF Draft #2 or later specifications.
3	CHAP-Password	PPP (Point-to-Point Protocol) CHAP (Challenge Handshake Authentication Protocol) response to an Access-Challenge.
4	NAS-IP Address	IP address of the AAA client that is requesting authentication.
5	NAS-Port	Physical port number of the AAA client that is authenticating the user. The AAA client port value (32 bits) consists of one or two 16-bit values, depending on the setting of the RADIUS server extended **portnames** command. Each 16-bit number is a 5-digit decimal integer interpreted as follows: For asynchronous terminal lines, async network interfaces, and virtual async interfaces, the value is **00***ttt*, where *ttt* is the line number or async interface unit number. For ordinary synchronous network interfaces, the value is **10xxx**. For channels on a primary-rate ISDN (Integrated Services Digital Network) interface, the value is **2ppcc**. For channels on a basic rate ISDN interface, the value is **3bb0c**. For other types of interfaces, the value is **6nnss**.

Downloaded from www.Manualslib.com manuals search engine

Table D-7 RADIUS (IETF) Attributes (continued)

No.	Attribute	Description
6	Service-Type	Type of service requested or type of service to be provided: In a request: **Framed—**For known PPP or SLIP (Serial Line Internet Protocol) connection. **Administrative User—**For **enable** command. In a response: **Login—**Make a connection. **Framed—**Start SLIP or PPP. **Administrative User—**Start an EXEC or **enable ok**. **Exec User—**Start an EXEC session.
7	Framed-Protocol	Framing to be used for framed access.
8	Framed-IP-Address	Address to be configured for the user.
9	Framed-IP-Netmask	IP netmask to be configured for the user when the user is a router to a network. This attribute-value results in a static route being added for Framed-IP-Address with the mask specified.
10	Framed-Routing	Routing method for the user when the user is a router to a network. Only None and Send and Listen values are supported for this attribute.
11	Filter-Id	Name of the filter list for the user, formatted as follows: %d, %d.in, or %d.out. This attribute is associated with the most recent service-type command. For login and EXEC, use %d or %d.out as the line access list value from 0 to 199. For Framed service, use %d or %d.out as interface output access list and %d.in for input access list. The numbers are self-encoding to the protocol to which they refer.
12	Framed-MTU	Indicates the maximum transmission unit (MTU) that can be configured for the user when the MTU is not negotiated by PPP or some other means.
13	Framed-Compression	Compression protocol used for the link. This attribute results in "/compress" being added to the PPP or SLIP autocommand generated during EXEC authorization. Not currently implemented for non-EXEC authorization.

Downloaded from www.Manualslib.com manuals search engine

Table D-7 RADIUS (IETF) Attributes (continued)

No.	Attribute	Description
14	Login-IP-Host	Host to which the user will connect when the Login-Service attribute is included.
15	Login-Service	Service that should be used to connect the user to the login host. Service is indicated by a numeric value as follows: 0: Telnet 1: Rlogin 2: TCP-Clear 3: PortMaster 4: LAT
16	Login-TCP-Port	TCP (Transmission Control Protocol) port with which the user is to be connected when the Login-Service attribute is also present.
18	Reply-Message	Text to be displayed to the user.
22	Framed-Route	Routing information to be configured for the user on this AAA client. The RADIUS RFC (Request for Comments) format (net/bits [router [metric]]) and the old style dotted mask (net mask [router [metric]]) are supported. If the router field is omitted or 0 (zero), the peer IP address is used. Metrics are currently ignored.
24	State	Allows State information to be maintained between the AAA client and the RADIUS server. This attribute is applicable only to CHAP challenges.

Downloaded from www.Manualslib.com manuals search engine

Table D-7 RADIUS (IETF) Attributes (continued)

No.	Attribute	Description

26	Vendor-Specific	Allows vendors to support their own extended attributes. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option is vendor-type 1, cisco-avpair. The value is a string of the format:
		protocol:attribute sep value
		
		Protocol is a value of the Cisco protocol attribute for a particular type of authorization. Attribute and value are an appropriate AV pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes. This allows the full set of TACACS+ authorization features to be used for RADIUS. The following is an example:
		`cisco-avpair= "ip:addr-pool=first"`
		`cisco-avpair= "shell:priv-lvl=15"`
		
		The first example causes Cisco's multiple named IP address pools feature to be activated during IP authorization (during PPP's IPCP address assignment). The second example causes a AAA client prompt user to have immediate access to EXEC commands.

27	Session-Timeout	Maximum number of seconds of service to be provided to the user before the session terminates. This attribute value becomes the per-user absolute timeout. This attribute is not valid for PPP sessions.
28	Idle-Timeout	Maximum number of consecutive seconds of idle connection time allowed to the user before the session terminates. This attribute value becomes the per-user session-timeout. This attribute is not valid for PPP sessions.
34	Login-LAT-Service	System with which the user is to be connected by LAT. This attribute is only available in the EXEC mode.

Downloaded from www.Manualslib.com manuals search engine

Table D-7 RADIUS (IETF) Attributes (continued)

No.	Attribute	Description
61	NAS-Port-Type	Indicates the type of physical port the AAA client is using to authenticate the user. Physical ports are indicated by a numeric value as follows: 0: Asynchronous 1: Synchronous 2: ISDN-Synchronous 3: ISDN-Asynchronous (V.120) 4: ISDN- Asynchronous (V.110) 5: Virtual
62	Port-Limit	Sets the maximum number of ports to be provided to the user by the network access server.

RADIUS (IETF) Accounting AV Pairs

Table D-8 lists the supported RADIUS (IETF) accounting attributes. If the attribute has a security server-specific format, the format is specified.

Table D-8 RADIUS (IETF) Accounting Attributes

No.	Attribute	Description
25	Class	Arbitrary value that the AAA client includes in all accounting packets for this user if supplied by the RADIUS server.
30	Called-Station-Id	Allows the AAA client to send the telephone number the user called into as part of the access-request packet, using DNIS (Dialed Number Identification Server) or similar technology. This attribute is only supported on ISDN and for modem calls on the Cisco AS5200 if used with PRI (Primary Rate Interface).

Downloaded from www.Manualslib.com manuals search engine

Table D-8 RADIUS (IETF) Accounting Attributes (continued)

No.	Attribute	Description
31	Calling-Station-Id	Allows the AAA client to send the telephone number the call came from as part of the access-request packet using automatic number identification or similar technology. This attribute has the same value as remote-addr in TACACS+. This attribute is supported only on ISDN and for modem calls on the Cisco AS5200 if used with PRI.
40	Acct-Status-Type	Specifies whether this accounting-request marks the beginning of the user service (start) or the end (stop).
41	Acct-Delay-Time	Number of seconds the client has been trying to send a particular record.
42	Acct-Input-Octets	Number of octets received from the port while this service is being provided.
43	Acct-Output-Octets	Number of octets sent to the port while this service is being delivered.
44	Acct-Session-Id	Unique accounting identifier that makes it easy to match start and stop records in a log file. The Acct-Session-Id restarts at 1 each time the router is power cycled or the software is reloaded. Contact Cisco support if this is unsuitable.
45	Acct-Authentic	Way in which the user was authenticated—by RADIUS, by the AAA client itself, or by another remote authentication protocol. This attribute is set to **radius** for users authenticated by RADIUS; to **remote** for TACACS+ and Kerberos; or to **local** for local, enable, line, and if-needed methods. For all other methods, the attribute is omitted.
46	Acct-Session-Time	Number of seconds the user has been receiving service.
47	Acct-Input-Packets	Number of packets received from the port while this service is being provided to a framed user.
48	Acct-Output-Packets	Number of packets sent to the port while this service is being delivered to a framed user.

Downloaded from www.Manualslib.com manuals search engine

Table D-8 RADIUS (IETF) Accounting Attributes (continued)

No.	Attribute	Description
49	Acct-Terminate-Cause	Reports details on why the connection was terminated. Termination causes are indicated by a numeric value as follows: 1: User request 2: Lost carrier 3: Lost service 4: Idle timeout 5: Session-timeout 6: Admin reset 7: Admin reboot 8: Port error 9: AAA client error 10: AAA client request 11: AAA client reboot 12: Port unneeded 13: Port pre-empted 14: Port suspended 15: Service unavailable 16: Callback 17: User error 18: Host request
61	NAS-Port-Type	Type of physical port the AAA client is using to authenticate the user.

Microsoft MPPE Dictionary of RADIUS VSAs

Cisco Secure ACS supports the Microsoft RADIUS VSAs used for Microsoft Point-to-Point Encryption (MPPE). The vendor ID for this Microsoft RADIUS Implementation is 311. MPPE is an encryption technology developed by

Downloaded from www.Manualslib.com manuals search engine

Microsoft to encrypt point-to-point (PPP) links. These PPP connections can be via a dial-up line, or over a VPN tunnel such as PPTP. MPPE is supported by several RADIUS network device vendors that Cisco Secure ACS supports. The following Cisco Secure ACS RADIUS protocols support the Microsoft RADIUS VSAs:

- Cisco IOS
- Cisco VPN 3000
- Ascend

Table D-9 lists the supported MPPE RADIUS VSAs.

Table D-9 Microsoft MPPE RADIUS VSAs

Attribute	Number	Type of Value	Description
MS-CHAP-Response	1	string	—
MS-CHAP-Error	2	string	—
MS-CHAP-CPW-1	3	string	—
MS-CHAP-CPW-2	4	string	—
MS-CHAP-LM-Enc-PW	5	string	—
MS-CHAP-NT-Enc-PW	6	string	—
MS-MPPE-Encryption-Policy	7	integer	The MS-MPPE-Encryption-Policy attribute signifies whether the use of encryption is allowed or required. If the Policy field is equal to 1 (Encryption-Allowed), any or none of the encryption types specified in the MS-MPPE-Encryption-Types attribute can be used. If the Policy field is equal to 2 (Encryption-Required), any of the encryption types specified in the MS-MPPE-Encryption-Types attribute can be used, but at least one must be used.
MS-MPPE-Encryption-Types	8	integer	The MS-MPPE-Encryption-Types attribute signifies the types of encryption available for use with MPPE. It is a four octet integer that is interpreted as a string of bits.

Downloaded from www.Manualslib.com manuals search engine

Table D-9 Microsoft MPPE RADIUS VSAs (continued)

Attribute	Number	Type of Value	Description
MS-CHAP-Domain	10	string	—
MS-CHAP-Challenge	11	string	—
MS-CHAP-MPPE-Keys	12	string	The MS-CHAP-MPPE-Keys attribute contains two session keys for use by the MPPE. This attribute is only included in Access-Accept packets. The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.
MS-MPPE-Send-Key	16	string	The MS-MPPE-Send-Key attribute contains a session key for use by MPPE. As the name implies, this key is intended for encrypting packets sent from the AAA client to the remote host. This attribute is only included in Access-Accept packets.
MS-MPPE-Recv-Key	17	string	The MS-MPPE-Recv-Key attribute contains a session key for use by MPPE. As the name implies, this key is intended for encrypting packets received by the AAA client from the remote host. This attribute is only included in Access-Accept packets
MS-RAS-Version	18	string	—
MS-CHAP-NT-Enc-PW	25	string	—
MS-CHAP2-Response	26	string	—
MS-CHAP2-CPW	27	string	—

Downloaded from www.Manualslib.com manuals search engine

Ascend Dictionary of RADIUS AV Pairs

Cisco Secure ACS supports the Ascend RADIUS AV pairs. Table D-10 contains Ascend RADIUS dictionary translations for parsing requests and generating responses. All transactions are composed of AV pairs. The value of each attribute is specified as one of the following valid data types:

- **string—**0-253 octets
- **abinary—**0-254 octets
- **ipaddr—**4 octets in network byte order
- **integer—**32-bit value in big endian order (high byte first)
- **call filter—**Defines a call filter for the profile

Note RADIUS filters are retrieved only when a call is placed using a RADIUS outgoing profile or answered using a RADIUS incoming profile. Filter entries are applied in the order in which they are entered. If you make changes to a filter in an Ascend RADIUS profile, the changes do not take effect until a call uses that profile.

- **date—**32-bit value in big-endian order. For example, seconds since 00:00:00 universal time (UT), January 1, 1970
- **enum**—Enumerated values are stored in the user file with dictionary value translations for easy administration.

Table D-10 Ascend RADIUS Attributes

Attribute	Number	Type of Value
Dictionary of Ascend Attributes		
User-Name	1	string
Password	2	string
Challenge-Response	3	string
NAS-Identifier	4	ipaddr
NAS-Port	5	integer
User-Service	6	integer

Downloaded from www.Manualslib.com manuals search engine

Table D-10 Ascend RADIUS Attributes (continued)

Attribute	Number	Type of Value
Framed-Protocol	7	integer
Framed-Address	8	ipaddr
Framed-Netmask	9	ipaddr
Framed-Routing	10	integer
Framed-Filter	11	string
Framed-MTU	12	integer
Framed-Compression	13	integer
Login-Host	14	ipaddr
Login-Service	15	integer
Login-TCP-Port	16	integer
Change-Password	17	string
Reply-Message	18	string
Callback-Number	19	string
Callback-Name	20	string
Framed-Route	22	string
Framed-IPX-Network	23	integer
State	24	string
Class	25	string
Vendor-Specific	26	string
Client-Port-DNIS	30	string
Caller-Id	31	string
Acct-Status-Type	40	integer
Acct-Delay-Time	41	integer
Acct-Input-Octets	42	integer
Acct-Output-Octets	43	integer
Acct-Session-Id	44	integer
Acct-Authentic	45	integer

Downloaded from www.Manualslib.com manuals search engine

Table D-10 Ascend RADIUS Attributes (continued)

Attribute	Number	Type of Value
Acct-Session-Time	46	integer
Acct-Input-Packets	47	integer
Acct-Output-Packets	48	integer
Tunnel-Type	64	string
Tunnel-Medium-Type	65	string
Tunnel-Client-Endpoint	66	string
Tunnel-Server-Endpoint	67	string
Tunnel-ID	68	integer
Ascend-Private-Route	104	string
Ascend-Numbering-Plan-ID	105	integer
Ascend-FR-Link-Status-Dlci	106	integer
Ascend-Calling-Subaddress	107	string
Ascend-Callback-Delay	108	string
Ascend-My-Name-Alias	109	string
Ascend-Remote-FW	110	string
Ascend-Multicast-GLeave-Delay	111	integer
Ascend-CBCP-Enable	112	string
Ascend-CBCP-Mode	113	string
Ascend-CBCP-Delay	114	string
Ascend-CBCP-Trunk-Group	115	string
Ascend-AppleTalk-Route	116	string
Ascend-AppleTalk-Peer-Mode	117	string
Ascend-Route-AppleTalk	118	string
Ascend-FCP-Parameter	119	string
Ascend-Modem-PortNo	120	integer
Ascend-Modem-SlotNo	121	integer
Ascend-Modem-ShelfNo	122	integer

Downloaded from www.Manualslib.com manuals search engine

Table D-10 Ascend RADIUS Attributes (continued)

Attribute	Number	Type of Value
Ascend-Call-Attempt-Limit	123	integer
Ascend-Call-Block_Duration	124	integer
Ascend-Maximum-Call-Duration	125	integer
Ascend-Router-Preference	126	string
Ascend-Tunneling-Protocol	127	string
Ascend-Shared-Profile-Enable	128	string
Ascend-Primary-Home-Agent	129	string
Ascend-Secondary-Home-Agent	130	string
Ascend-Dialout-Allowed	131	integer
Ascend-BACP-Enable	133	string
Ascend-DHCP-Maximum-Leases	134	integer
Ascend-Client-Primary-DNS	135	address
Ascend-Client-Secondary-DNS	136	address
Ascend-Client-Assign-DNS	137	enum
Ascend-User-Acct-Type	138	enum
Ascend-User-Acct-Host	139	address
Ascend-User-Acct-Port	140	integer
Ascend-User-Acct-Key	141	string
Ascend-User-Acct-Base	142	enum
Ascend-User-Acct-Time	143	integer
Support IP Address Allocation from Global Pools		
Ascend-Assign-IP-Client	144	ipaddr
Ascend-Assign-IP-Server	145	ipaddr
Ascend-Assign-IP-Global-Pool	146	string
DHCP Server Functions		
Ascend-DHCP-Reply	147	integer
Ascend-DHCP-Pool-Number	148	integer

Downloaded from www.Manualslib.com manuals search engine

Table D-10 Ascend RADIUS Attributes (continued)

Attribute	Number	Type of Value
Connection Profile/Telco Option		
Ascend-Expect-Callback	149	integer
Event Type for an Ascend-Event Packet		
Ascend-Event-Type	150	integer
RADIUS Server Session Key		
Ascend-Session-Svr-Key	151	string
Multicast Rate Limit Per Client		
Ascend-Multicast-Rate-Limit	152	integer
Connection Profile Fields to Support Interface-Based Routing		
Ascend-IF-Netmask	153	ipaddr
Ascend-Remote-Addr	154	ipaddr
Multicast Support		
Ascend-Multicast-Client	155	integer
Frame Datalink Profiles		
Ascend-FR-Circuit-Name	156	string
Ascend-FR-LinkUp	157	integer
Ascend-FR-Nailed-Group	158	integer
Ascend-FR-Type	159	integer
Ascend-FR-Link-Mgt	160	integer
Ascend-FR-N391	161	integer
Ascend-FR-DCE-N392	162	integer
Ascend-FR-DTE-N392	163	integer
Ascend-FR-DCE-N393	164	integer
Ascend-FR-DTE-N393	165	integer
Ascend-FR-T391	166	integer
Ascend-FR-T392	167	integer
Ascend-Bridge-Address	168	string

Downloaded from www.Manualslib.com manuals search engine

Table D-10 Ascend RADIUS Attributes (continued)

Attribute	Number	Type of Value
Ascend-TS-Idle-Limit	169	integer
Ascend-TS-Idle-Mode	170	integer
Ascend-DBA-Monitor	171	integer
Ascend-Base-Channel-Count	172	integer
Ascend-Minimum-Channels	173	integer
IPX Static Routes		
Ascend-IPX-Route	174	string
Ascend-FT1-Caller	175	integer
Ascend-Backup	176	string
Ascend-Call-Type	177	integer
Ascend-Group	178	string
Ascend-FR-DLCI	179	integer
Ascend-FR-Profile-Name	180	string
Ascend-Ara-PW	181	string
Ascend-IPX-Node-Addr	182	string
Ascend-Home-Agent-IP-Addr	183	ipaddr
Ascend-Home-Agent-Password	184	string
Ascend-Home-Network-Name	185	string
Ascend-Home-Agent-UDP-Port	186	integer
Ascend-Multilink-ID	187	integer
Ascend-Num-In-Multilink	188	integer
Ascend-First-Dest	189	ipaddr
Ascend-Pre-Input-Octets	190	integer
Ascend-Pre-Output-Octets	191	integer
Ascend-Pre-Input-Packets	192	integer
Ascend-Pre-Output-Packets	193	integer
Ascend-Maximum-Time	194	integer

Downloaded from www.Manualslib.com manuals search engine

Table D-10 Ascend RADIUS Attributes (continued)

Attribute	Number	Type of Value
Ascend-Disconnect-Cause	195	integer
Ascend-Connect-Progress	196	integer
Ascend-Data-Rate	197	integer
Ascend-PreSession-Time	198	integer
Ascend-Token-Idle	199	integer
Ascend-Token-Immediate	200	integer
Ascend-Require-Auth	201	integer
Ascend-Number-Sessions	202	string
Ascend-Authen-Alias	203	string
Ascend-Token-Expiry	204	integer
Ascend-Menu-Selector	205	string
Ascend-Menu-Item	206	string
RADIUS Password Expiration Options		
Ascend-PW-Warntime	207	integer
Ascend-PW-Lifetime	208	integer
Ascend-IP-Direct	209	ipaddr
Ascend-PPP-VJ-Slot-Comp	210	integer
Ascend-PPP-VJ-1172	211	integer
Ascend-PPP-Async-Map	212	integer
Ascend-Third-Prompt	213	string
Ascend-Send-Secret	214	string
Ascend-Receive-Secret	215	string
Ascend-IPX-Peer-Mode	216	integer
Ascend-IP-Pool-Definition	217	string
Ascend-Assign-IP-Pool	218	integer
Ascend-FR-Direct	219	integer
Ascend-FR-Direct-Profile	220	string

Downloaded from www.Manualslib.com manuals search engine

Table D-10 Ascend RADIUS Attributes (continued)

Attribute	Number	Type of Value
Ascend-FR-Direct-DLCI	221	integer
Ascend-Handle-IPX	222	integer
Ascend-Netware-Timeout	223	integer
Ascend-IPX-Alias	224	integer
Ascend-Metric	225	integer
Ascend-PRI-Number-Type	226	integer
Ascend-Dial-Number	227	string
Connection Profile/PPP Options		
Ascend-Route-IP	228	integer
Ascend-Route-IPX	229	integer
Ascend-Bridge	230	integer
Ascend-Send-Auth	231	integer
Ascend-Send-Passwd	232	string
Ascend-Link-Compression	233	integer
Ascend-Target-Util	234	integer
Ascend-Max-Channels	235	integer
Ascend-Inc-Channel-Count	236	integer
Ascend-Dec-Channel-Count	237	integer
Ascend-Seconds-Of-History	238	integer
Ascend-History-Weigh-Type	239	integer
Ascend-Add-Seconds	240	integer
Ascend-Remove-Seconds	241	integer
Connection Profile/Session Options		
Ascend-Data-Filter	242	call filter
Ascend-Call-Filter	243	call filter
Ascend-Idle-Limit	244	integer
Ascend-Preempt-Limit	245	integer

Downloaded from www.Manualslib.com manuals search engine

Table D-10 Ascend RADIUS Attributes (continued)

Attribute	Number	Type of Value
Connection Profile/Telco Options		
Ascend-Callback	246	integer
Ascend-Data-Svc	247	integer
Ascend-Force-56	248	integer
Ascend-Billing-Number	249	string
Ascend-Call-By-Call	250	integer
Ascend-Transit-Number	251	string
Terminal Server Attributes		
Ascend-Host-Info	252	string
PPP Local Address Attribute		
Ascend-PPP-Address	253	ipaddr
MPP Percent Idle Attribute		
Ascend-MPP-Idle-Percent	254	integer
Ascend-Xmit-Rate	255	integer

Nortel Dictionary of RADIUS VSAs

Table D-11 lists the Nortel RADIUS VSAs supported by Cisco Secure ACS. The Nortel vendor ID number is 1584.

Table D-11 Nortel RADIUS VSAs

Attribute	Number	Type of Value
Bay-Local-IP-Address	035	ipaddr
Bay-Primary-DNS-Server	054	ipaddr
Bay-Secondary-DNS-Server	055	ipaddr
Bay-Primary-NBNS-Server	056	ipaddr
Bay-Secondary-NBNS-Server	057	ipaddr

Downloaded from www.Manualslib.com manuals search engine

Table D-11 Nortel RADIUS VSAs

Attribute	Number	Type of Value
Bay-User-Level	100	integer
Bay-Audit-Level	101	integer

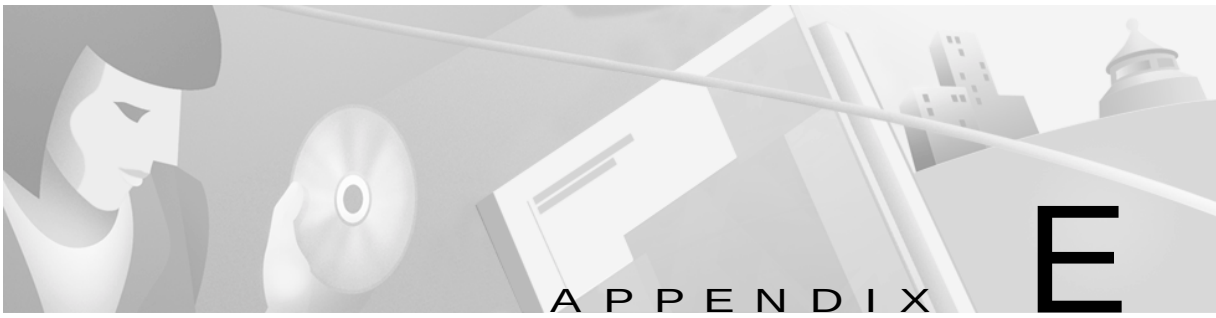
Juniper Dictionary of RADIUS VSAs

Table D-12 lists the Juniper RADIUS VSAs supported by Cisco Secure ACS. The Juniper vendor ID number is 2636.

Table D-12 Juniper RADIUS VSAs

Attribute	Number	Type of Value
Juniper-Local-User-Name	001	string
Juniper-Allow-Commands	002	string
Juniper-Deny-Commands	003	string

Downloaded from www.Manualslib.com manuals search engine



Cisco Secure ACS Command-Line Database Utility

This appendix details the Cisco Secure ACS command-line utility, CSUtil.exe. Among its several functions, CSUtil.exe enables you to add, change, and delete users from a colon-delimited text file. You can also use the utility to add and delete AAA client configurations.

Note You can accomplish similar tasks using the ACS System Backup, ACS System Restore, Database Replication, and RDBMS Synchronization features. For more information on these features, see Chapter 8, "Establishing Cisco Secure ACS System Configuration."

This appendix contains the following topics:

- Location of CSUtil.exe and Related Files, page E-2
- CSUtil.exe Syntax, page E-2
- CSUtil.exe Options, page E-3
- Backing Up Cisco Secure ACS with CSUtil.exe, page E-5
- Restoring Cisco Secure ACS with CSUtil.exe, page E-6
- Creating a CiscoSecure User Database, page E-7
- Creating a Cisco Secure ACS Database Dump File, page E-9
- Loading the Cisco Secure ACS Database from a Dump File, page E-10
- Compacting the CiscoSecure User Database, page E-11

Downloaded from www.Manualslib.com manuals search engine

- User and AAA Client Import Option, page E-13
- Exporting User List to a Text File, page E-23
- Exporting Group Information to a Text File, page E-24
- Exporting Registry Information to a Text File, page E-25
- Decoding Error Numbers, page E-25
- Recalculating CRC Values, page E-26
- User-Defined RADIUS Vendors and VSA Sets, page E-27

Location of CSUtil.exe and Related Files

When you install Cisco Secure ACS in the default location, CSUtil.exe is located in the following directory:

`C:\Program Files\CiscoSecure ACS v`*`X.X`*`\Utils`

where *X.X* is the version of your Cisco Secure ACS software. Regardless of where you install Cisco Secure ACS, CSUtil.exe is located in the `Utils` directory.

Files generated by or accessed by `CSUtil.exe` are also located in the `Utils` directory.

CSUtil.exe Syntax

The syntax for the CSUtil.exe command is as follows:

`CSUtil.exe [-q] [-c] [-d] [-g] [-i` *`filename`*`] [[-p] -l` *`filename`*`] [-e` *`-number`*`] [-b` *`filename`*`] [-r` *`filename`*`] [-f] [-n] [-u] [-y] [-listUDV] [-addUDV` *`slotfilename`*`] [-delUDV` *`slot`*`]`

Note Most CSUtil.exe options require that you stop the CSAuth service. While the CSAuth service is stopped, Cisco Secure ACS does not authenticate users. To determine if an option requires that you stop CSAuth, see the "CSUtil.exe Options" section on page E-3.

Downloaded from www.Manualslib.com manuals search engine

You can combine many of the options in a single use of CSUtil.exe. If you are new to using CSUtil.exe, we recommend performing only one option at a time, with the exception of those options, such as -p, that must be used in conjunction with other options.

Experienced CSUtil.exe users may find it useful to combine CSUtil.exe options, such as the following example, which would first import AAA client configurations and then generate a dump of all Cisco Secure ACS internal data:

```
CSUtil.exe -i newnases.txt -d
```

CSUtil.exe Options

CSUtil.exe can perform several actions. The options, listed below in alphabetical order, are detailed in later sections of this chapter.

- **-b—**Backup system to a specified filename. For more information about this option, see the "Backing Up Cisco Secure ACS with CSUtil.exe" section on page E-5.
- **-c—**Recalculate database CRC values. For more information about this option, see the "Recalculating CRC Values" section on page E-26.
- **-d—**Export all Cisco Secure ACS internal data to a file named `dump.txt`. Using this option requires that you stop the CSAuth service. For more information about this option, see the "Creating a Cisco Secure ACS Database Dump File" section on page E-9.
- **-e—**Decode internal Cisco Secure ACS error numbers to ASCII message. For more information about this option, see the "Decoding Error Numbers" section on page E-25.
- **-g—**Export group information to a file named `groups.txt`. Using this option requires that you stop the CSAuth service. For more information about this option, see the "Exporting Group Information to a Text File" section on page E-24.
- **-i—**Import user or AAA client information from a file named `import.txt` or a specified file. For more information about this option, see the "Importing User and AAA Client Information" section on page E-13.

Downloaded from www.Manualslib.com manuals search engine

- **-l—**Load all Cisco Secure ACS internal data from a file named `dump.txt` or named file. Using this option requires that you stop the CSAuth service. For more information about this option, see the "Loading the Cisco Secure ACS Database from a Dump File" section on page E-10.
- **-n—**Create CiscoSecure user database and index. Using this option requires that you stop the CSAuth service. For more information about this option, see the "Creating a CiscoSecure User Database" section on page E-7.
- **-p—**Reset password aging counters during database load, to be used only in conjunction with the -l option. For more information about this option, see the "Loading the Cisco Secure ACS Database from a Dump File" section on page E-10.
- **-q—**Run CSUtil.exe without confirmation prompts.
- **-r—**Restore system from a specified backup filename. For more information about this option, see the "Restoring Cisco Secure ACS with CSUtil.exe" section on page E-6.
- **-u—**Export user information, sorted by group membership, to a file named `users.txt`. Using this option requires that you stop the CSAuth service. For more information about this option, see the "Exporting User List to a Text File" section on page E-23.
- **-y—**Dump Windows NT/2000 Registry configuration information to a file named `setup.txt`. For more information about this option, see the "Exporting Registry Information to a Text File" section on page E-25.
- **-addUDV**—Add a user-defined RADIUS vendor-specific attribute (VSA). For more information about this option, see the "Adding a Custom RADIUS Vendor and VSA Set" section on page E-28.
- **-delUDV**—Delete a user-defined RADIUS VSA. For more information about this option, see the "Deleting a Custom RADIUS Vendor and VSA Set" section on page E-29.
- **-listUDV**—List all user-defined RADIUS VSAs currently defined in Cisco Secure ACS. For more information about this option, see the "Listing Custom RADIUS Vendors" section on page E-30.

Downloaded from www.Manualslib.com manuals search engine

Backing Up Cisco Secure ACS with CSUtil.exe

You can use the -b option to create a system backup of all Cisco Secure ACS internal data. The resulting backup file has the same data as the backup files produced by the ACS Backup feature found in the HTML interface. For more information about the ACS Backup feature, see the "Cisco Secure ACS Backup" section on page 8-40.

Note During the backup, all services are automatically stopped and restarted. No users are authenticated while the backup is occurring.

To back up Cisco Secure ACS with CSUtil.exe, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 2 Type:

```
CSUtil.exe -b  filename
```

where *filename* is the name of the backup file. Press **Enter**.

Result: CSUtil.exe displays a confirmation prompt.

Step 3 To confirm that you want to perform a backup and to halt all Cisco Secure ACS services during the backup, type **Y** and press **Enter**.

Result: CSUtil.exe generates a complete backup of all Cisco Secure ACS internal data, including user accounts and system configuration. This process may take a few minutes.

Note CSUtil.exe displays the error message `Backup Failed` when it attempts to backup components of Cisco Secure ACS that are empty, such as when no administrator accounts exist. These apply only to the components that are empty, not to the overall success or failure of the backup.

Downloaded from www.Manualslib.com manuals search engine

Restoring Cisco Secure ACS with CSUtil.exe

You can use the -r option to restore all Cisco Secure ACS internal data. The backup file from which you restore Cisco Secure ACS can be one generated by the CSUtil.exe -b option or by the ACS Backup feature in the HTML interface.

Cisco Secure ACS backup files contain two types of data:

- User and group data
- System configuration

You can restore either user and group data or system configuration, or both. For more information about the ACS Backup feature, see the "Cisco Secure ACS Backup" section on page 8-40.

Note During the backup, all services are automatically stopped and restarted. No users are authenticated while the restoration is occurring.

To restore Cisco Secure ACS with CSUtil.exe, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 2 Perform the applicable restoration command:

a. To restore all data (user and group data, and system configuration), type:

```
CSUtil.exe -r all  filename
```

where *filename* is the name of the backup file. Press **Enter**.

b. To restore only user and group data, type:

```
CSUtil.exe -r users  filename
```

where *filename* is the name of the backup file. Press **Enter**.

Downloaded from www.Manualslib.com manuals search engine

c. To restore only the system configuration, type:

```
CSUtil.exe -r config filename
```

where *filename* is the name of the backup file. Press **Enter**.

Result: CSUtil.exe displays a confirmation prompt.

Step 3 To confirm that you want to perform a restoration and to halt all Cisco Secure ACS services during the restoration, type **Y** and press **Enter**.

Result: CSUtil.exe restores the specified portions of your Cisco Secure ACS data. This process may take a few minutes.

Note If the backup file is missing a database component, CSUtil.exe displays an error message. Such an error message applies only to the restoration of the missing component. The absence of a database component in a backup is usually intentional and indicates that the component was empty in Cisco Secure ACS at the time the backup was created.

Creating a CiscoSecure User Database

You can use the -n option to create a CiscoSecure user database.

Note Using the -n option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

Caution Using the -n option erases all user information in the CiscoSecure user database. Unless you have a current backup or dump of your CiscoSecure user database, all user accounts are lost when you use this option.

Downloaded from www.Manualslib.com manuals search engine

To create a CiscoSecure user database, follow these steps:

Step 1 If you have not performed a backup or dump of the CiscoSecure user database, do so now before proceeding. For more information about backing up the database, see the "Backing Up Cisco Secure ACS with CSUtil.exe" section on page E-5.

Step 2 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 3 If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

Result: The CSAuth service stops.

Step 4 Type:

```
CSUtil.exe -n
```

and press **Enter**.

Result: CSUtil.exe displays a confirmation prompt.

Step 5 To confirm that you want to initialize the CiscoSecure user database, type **Y** and press **Enter**.

Result: The CiscoSecure user database is initialized. This process may take a few minutes.

Step 6 To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

Downloaded from www.Manualslib.com manuals search engine

Creating a Cisco Secure ACS Database Dump File

You can use the -d option to dump all the contents of the CiscoSecure user database into a text file. In addition to providing a thorough, eye-readable, and compressible backup of all Cisco Secure ACS internal data, a database dump can also be useful for the Cisco Technical Assistance Center (TAC) during troubleshooting.

Using the -l option, you can reload the Cisco Secure ACS internal data from a dump file created by the -d option. For more information about the -l option, see the "Loading the Cisco Secure ACS Database from a Dump File" section on page E-10.

Note Using the -d option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To dump all Cisco Secure ACS internal data into a text file, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 2 If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

Result: The CSAuth service stops.

Step 3 Type:

```
CSUtil.exe -d
```

Press **Enter**.

Result: CSUtil.exe displays a confirmation prompt.

Downloaded from www.Manualslib.com manuals search engine

Step 4 To confirm that you want to dump all Cisco Secure ACS internal data into `dump.txt`, type **Y** and press **Enter**.

Result: CSUtil.exe creates the `dump.txt` file. This process may take a few minutes.

Step 5 To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

Loading the Cisco Secure ACS Database from a Dump File

You can use the -l option to overwrite all Cisco Secure ACS internal data from a dump text file. This option replaces the existing all Cisco Secure ACS internal data with the data in the dump text file. In effect, the -l option initializes all Cisco Secure ACS internal data before loading it from the dump text file. Dump text files are created using the -d option. While the -d option only produces dump text files that are named `dump.txt`, the -l option allows for loading renamed dump files. For more information about creating dump text files, see the "Creating a Cisco Secure ACS Database Dump File" section on page E-9.

You can use the -p option in conjunction with the -l option to reset password-aging counters.

Note Using the -l option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To load all Cisco Secure ACS internal data from a text file, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Downloaded from www.Manualslib.com manuals search engine

Step 2 If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

Result: The CSAuth service stops.

Step 3 Type:

```
CSUtil.exe -l filename
```

where *filename* is the name of the dump file you want CSUtil.exe to use to load Cisco Secure ACS internal data. Press **Enter**.

Result: CSUtil.exe displays a confirmation prompt for overwriting all Cisco Secure ACS internal data with the data in the dump text file.

Note Overwriting the database does not preserve any data; instead, after the overwrite, the database contains only what is specified in the dump text file.

Step 4 To confirm that you want to replace all Cisco Secure ACS internal data, type **Y** and press **Enter**.

Result: CSUtil.exe initializes all Cisco Secure ACS internal data, and then loads Cisco Secure ACS with the information in the dump file specified. This process may take a few minutes.

Step 5 To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

Compacting the CiscoSecure User Database

Like many relational databases, the CiscoSecure user database handles the deletion of records by marking deleted records as deleted but not removing the record from the database. Over time, your CiscoSecure user database may be substantially larger than is required by the number of users it contains. To reduce the CiscoSecure user database size, you can compact it periodically.

Downloaded from www.Manualslib.com manuals search engine

Compacting the CiscoSecure user database consists of using in conjunction three CSUtil.exe options:

- **-d—**Export all Cisco Secure ACS internal data to a text file named `dump.txt`.
- **-n—**Create a CiscoSecure user database and index.
- **-l—**Load all Cisco Secure ACS internal data from a text file. If you do not specify the file name, CSUtil.exe uses the default file name `dump.txt`.

Additionally, if you want to automate this process, consider using the -q option to suppress the confirmation prompts that otherwise appear before CSUtil.exe performs the -n and -l options.

Note Compacting the CiscoSecure user database requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To compact the CiscoSecure user database, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 2 If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

Result: The CSAuth service stops.

Step 3 Type:

```
CSUtil.exe -d -n -l
```

Press **Enter**.

Tip If you include the -q option in the command, CSUtil.exe does not prompt you for confirmation of initializing or loading the database.

Downloaded from www.Manualslib.com manuals search engine

Result: If you do not use the -q option, CSUtil.exe displays a confirmation prompt for initializing the database and then for loading the database. For more information about the effects of the -n option, see the "Creating a CiscoSecure User Database" section on page E-7. For more information about the effects of the -l option, see the "Loading the Cisco Secure ACS Database from a Dump File" section on page E-10.

Step 4 For each confirmation prompt that appears, type **Y** and press **Enter**.

Result: CSUtil.exe dumps all Cisco Secure ACS internal data to `dump.txt`, initializes the CiscoSecure user database, and reloads all Cisco Secure ACS internal data from `dump.txt`. This process may take a few minutes.

Step 5 To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

User and AAA Client Import Option

The -i option enables you to update Cisco Secure ACS with data from a colon-delimited text file. You can also update AAA client definitions.

For user accounts, you can add users, change user information, or delete users. For AAA client definitions, you can add or delete AAA clients.

This section contains the following topics:

- Importing User and AAA Client Information, page E-13
- User and AAA Client Import File Format, page E-15

Importing User and AAA Client Information

To import user or AAA client information, follow these steps:

Step 1 If you have not performed a backup or dump of Cisco Secure ACS, do so now before proceeding. For more information about backing up the database, see the "Backing Up Cisco Secure ACS with CSUtil.exe" section on page E-5.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Create an import text file. For more information about what an import text file can or must contain, see the "User and AAA Client Import File Format" section on page E-15.

Step 3 Copy or move the import text file to the same directory as CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 4 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe.

Step 5 Type:

```
CSUtil.exe -i filename
```

where *filename* is the name of the import text file you want CSUtil.exe to use to update Cisco Secure ACS. Press **Enter**.

Result: CSUtil.exe displays a confirmation prompt for updating the database.

Step 6 To confirm that you want to update Cisco Secure ACS with the information from the import text file specified, type **Y** and press **Enter**.

Result: Cisco Secure ACS is updated with the information in the import text file specified. This process may take a few minutes.

If the import text file contained AAA client configuration data, CSUtil.exe warns you that you need to restart CSTacacs and CSRadius in order for these changes to take effect.

Step 7 To restart CSRadius, follow these steps:

a. Type:

```
net stop csradius
```

and press **Enter**.

Result: The CSRadius service stops.

b. To start CSRadius, type:

```
net start csradius
```

and press **Enter**.

Downloaded from www.Manualslib.com manuals search engine

Step 8 To restart CSTacacs, follow these steps:

a. Type:

```
net stop cstacacs
```

and press **Enter**.

Result: The CSTacacs service stops.

b. To start CSTacacs, type:

```
net start cstacacs
```

and press **Enter**.

User and AAA Client Import File Format

The import file can contain six different line types. At least two are required. This section contains an overview topic, topics for each of the six line types, and an example section:

- About User and AAA Client Import File Format, page E-15
- ONLINE or OFFLINE Statement, page E-16
- ADD Statements, page E-16
- UPDATE Statements, page E-18
- DELETE Statements, page E-20
- ADD_NAS Statements, page E-20
- DEL_NAS Statements, page E-22
- Import File Examples, page E-22

About User and AAA Client Import File Format

Each line of a CSUtil.exe import file is a series of colon-separated tokens. Some of the tokens are followed by values. Values, like tokens, are colon-delimited. For tokens that require values, CSUtil.exe expects the value of the token to be in the colon-delimited field immediately following the token.

Downloaded from www.Manualslib.com manuals search engine

ONLINE or OFFLINE Statement

CSUtil.exe requires an ONLINE or OFFLINE token in an import text file. The file must begin with a line that contains only a ONLINE or OFFLINE token. The ONLINE and OFFLINE tokens are described in Table E-1.

Table E-1 ONLINE/OFFLINE Statement Tokens

Token	Required	Value Required	Description
ONLINE	Either ONLINE or OFFLINE must be present	—	The CSAuth service remains active while CSUtil.exe imports the text file. CSUtil.exe performance is slower when run in this mode, but Cisco Secure ACS continues to authenticate users during the import.
OFFLINE	Either ONLINE or OFFLINE must be present	—	The CSAuth service is stopped while CSUtil.exe imports the text file. Although CSUtil.exe performance is fastest in this mode, no users are authenticated during the import. If you need to import a large amount of user information quickly, consider using the OFFLINE token. While performing an import in the OFFLINE mode stops authentication during the import, the import is much faster. For example, importing 100,000 users in the OFFLINE mode takes less than one minute.

ADD Statements

ADD statements are optional. Only the ADD token and its value are required to add a user to Cisco Secure ACS. The valid tokens for ADD statements are listed in Table E-2 on page E-17.

Note CSUtil.exe provides no means to specify a particular instance of an external user database type. If a user is to be authenticated by an external user database and Cisco Secure ACS has multiple instances of the specified database type, CSUtil.exe assigns the user to the first instance of that database type. For example, if Cisco Secure ACS has two LDAP external user databases configured, CSUtil.exe creates the user record and assigns the user to the LDAP database that was added to Cisco Secure ACS first.

Downloaded from www.Manualslib.com manuals search engine

Table E-2 ADD Statement Tokens

Token	Required	Value Required	Description
ADD	Yes	username	Add user information to Cisco Secure ACS. If the username already exists, no information is changed.
PROFILE	No	group number	Group number to which the user is assigned. This must be a number from 0 to 499, not a name. If you do not use the PROFILE token or fail to provide a group number, the user is added to the default group.
CHAP	No	CHAP password	Require a CHAP password for authentication.
SENDAUTH	No	sendauth password	Require a TACACS+ sendauth password.
CSDB	No	password	Authenticate the username with the CiscoSecure user database.
CSDB_UNIX	No	UNIX-encrypted password	Authenticate the username with the CiscoSecure user database, using a UNIX password format.
EXT_NT	No	—	Authenticate the username with a Windows NT/2000 external user database.
EXT_NDS	No	—	Authenticate the username with a Novell NDS external user database.
EXT_SDI	No	—	Authenticate the username with an RSA external user database.
EXT_ANPI	No	—	Authenticate the username with an AXENT external user database.
EXT_ CRYPTO	No	—	Authenticate the username with a CRYPTOCard external user database.
EXT_ODBC	No	—	Authenticate the username with an ODBC external user database.
EXT_LDAP	No	—	Authenticate the username with a generic LDAP external user database.
EXT_ ENIGMA	No	—	Authenticate the username with a SafeWord external user database.

Downloaded from www.Manualslib.com manuals search engine

Table E-2 ADD Statement Tokens (continued)

Token	Required	Value Required	Description
EXT_LEAP	No	—	Authenticate the username with a LEAP proxy RADIUS server external user database.
EXT_ACTV	No	—	Authenticate the username with an ActivCard external user database.
EXT_ VASCO	No	—	Authenticate the username with a Vasco external user database.
EXT_ RADIUS	No	—	Authenticate the username with a RADIUS token server external user database.

For example, the following ADD statement would create an account with the username "John", assign it to Group 3, and specify that John should be authenticated by the CiscoSecure user database with the password "closedmondays":

```
ADD:John:PROFILE:3:CSDB:closedmondays
```

UPDATE Statements

UPDATE statements are optional. They make changes to existing user accounts. Only the UPDATE token and its value are required by CSUtil.exe, but if no other tokens are included, no changes are made to the user account. The valid tokens for UPDATE statements are listed in Table E-3.

Table E-3 UPDATE Statement Tokens

Token	Required	Value Required	Description
UPDATE	Yes	username	Update user information to Cisco Secure ACS.
PROFILE	No	group number	Group number to which the user is assigned. This must be a number from 0 to 499, not a name.
CHAP	No	CHAP password	Require a CHAP password for authentication.
SENDAUTH	No	sendauth password	Require a TACACS+ sendauth password.

Downloaded from www.Manualslib.com manuals search engine

Table E-3 UPDATE Statement Tokens (continued)

Token	Required	Value Required	Description
CSDB	No	password	Authenticate the username with the CiscoSecure user database.
CSDB_UNIX	No	UNIX-encrypted password	Authenticate the username with the CiscoSecure user database, using a UNIX password format.
EXT_NT	No	—	Authenticate the username with a Windows NT/2000 external user database.
EXT_NDS	No	—	Authenticate the username with a Novell NDS external user database.
EXT_SDI	No	—	Authenticate the username with a RSA external user database.
EXT_ANPI	No	—	Authenticate the username with an AXENT external user database.
EXT_CRYPTO	No	—	Authenticate the username with a CRYPTOCard external user database.
EXT_ODBC	No	—	Authenticate the username with an ODBC external user database.
EXT_LDAP	No	—	Authenticate the username with a generic LDAP external user database.
EXT_ENIGMA	No	—	Authenticate the username with a SafeWord external user database.
EXT_LEAP	No	—	Authenticate the username with a LEAP proxy RADIUS server external user database.
EXT_ACTV	No	—	Authenticate the username with an ActivCard external user database.
EXT_VASCO	No	—	Authenticate the username with a Vasco external user database.
EXT_RADIUS	No	—	Authenticate the username with a RADIUS token server external user database.

Downloaded from www.Manualslib.com manuals search engine

For example, the following UPDATE statement causes CSUtil.exe to update the account with username "John", assign it to Group 50, specify that John should be authenticated by a UNIX-encrypted password, with a separate CHAP password "goodoldchap":

```
UPDATE:John:PROFILE:50:CSDB_UNIX:3Al3qf9:CHAP:goodoldchap
```

DELETE Statements

DELETE statements are optional. The DELETE token and its value are required to delete a user account from Cisco Secure ACS. The DELETE token, detailed in Table E-4, is the only token in a DELETE statement.

Table E-4 UPDATE Statement Tokens

Token	Required	Value Required	Description
DELETE	Yes	username	The name of the user account that is to be deleted.

For example, the following DELETE statement causes CSUtil.exe to permanently remove the account with username "John" from the CiscoSecure user database:

```
DELETE:John
```

ADD_NAS Statements

ADD_NAS statements are optional. The ADD_NAS, IP, KEY, and VENDOR tokens and their values are required to add a AAA client definition to Cisco Secure ACS. The valid tokens for ADD_NAS statements are listed in Table E-5.

Table E-5 ADD_NAS Statement Tokens

Token	Required	Value Required	Description
ADD_NAS	Yes	AAA client name	The name of the AAA client that is to be added.
IP	Yes	IP address	The IP address of the AAA client being added.
KEY	Yes	shared secret	The shared secret for the AAA client.

Downloaded from www.Manualslib.com manuals search engine

Table E-5 ADD_NAS Statement Tokens (continued)

Token	Required	Value Required	Description
VENDOR	Yes	See Description	The authentication protocol the AAA client uses. For RADIUS, this includes the VSA. The valid values are listed below. Quotation marks are required due to the spaces in the protocol names. "TACACS+ (Cisco IOS)" "RADIUS (IETF)" "RADIUS (Cisco IOS/PIX)" "RADIUS (Ascend)" "RADIUS (Cisco VPN 3000)" "RADIUS (Cisco VPN 5000)" "RADIUS (Cisco Aironet)" "RADIUS (Cisco BBSM)" "RADIUS (Nortel)" "RADIUS (Juniper)"
NDG	No	NDG name	The name of the Network Device Group to which the AAA client is to be added.
SINGLE_CON	No	Y or N	For AAA clients using TACACS+ only, the value set for this TOKEN specifies whether the Single Connect TACACS+ AAA Client option is enabled. For more information, see the "Adding and Configuring a AAA Client" section on page 4-9.
KEEPALIVE	No	Y or N	For AAA clients using TACACS+ only, the value set for this token specifies whether or not the Log Update/Watchdog Packets from this Access Server option is enabled. For more information, see the "Adding and Configuring a AAA Client" section on page 4-9.

Downloaded from www.Manualslib.com manuals search engine

For example, the following ADD_NAS statement causes CSUtil.exe to add a AAA client with the name "SVR2-T+", using TACACS+ with the single connection and keep alive packet options enabled:

```
ADD_NAS:SVR2-T+:IP:IP address:KEY:shared secret:VENDOR:"TACACS+ (Cisco
IOS)":NDG:"East Coast":SINGLE_CON:Y:KEEPALIVE:Y
```

DEL_NAS Statements

DEL_NAS statements are optional. The DEL_NAS token, detailed in Table E-6, is the only token in a DEL_NAS statement. DEL_NAS statements delete AAA client definitions from Cisco Secure ACS.

Table E-6 DEL_NAS Statement Tokens

Token	Required	Value Required	Description
DEL_NAS	Yes	AAA client name	The name of the AAA client that is to be deleted.

For example, the following DEL_NAS statement causes CSUtil.exe to delete a AAA client with the name "SVR2-T+":

```
DEL_NAS:SVR2-T+
```

Import File Examples

The following is an example import text file:

```
OFFLINE
ADD:user01:CSDB:userpassword:PROFILE:1
ADD:user02:EXT_NT:PROFILE:2
ADD:chapuser:CSDB:hello:CHAP:chappw:PROFILE:3
ADD:mary:EXT_NT:CHAP:achappassword
ADD:joe:EXT_SDI
ADD:vanessa:CSDB:vanessaspassword
ADD:juan:CSDB_UNIX:unixpassword
UPDATE:foobar:PROFILE:10
DELETE:paul
ADD_NAS:SVR2-T+:IP:209.165.202.136:KEY:A87il032bzg:VENDOR:"TACACS+
(Cisco IOS)":NDG:"East Coast"
DEL_NAS:SVR16-RAD
```


Downloaded from www.Manualslib.com manuals search engine

Exporting User List to a Text File

You can use the -u option to export a list of all users in the CiscoSecure user database to a text file named `users.txt`. The `users.txt` file organizes the users by group. Within each group, users are listed by the order of the creation of the user account in the CiscoSecure user database. For example, if accounts were created for Pat, Dana, and Lloyd, in that order, `users.txt` lists them in that order as well, rather than alphabetically.

Note Using the -u option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To export user information from the CiscoSecure user database into a text file, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 2 If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

Result: The CSAuth service stops.

Step 3 Type:

```
CSUtil.exe -u
```

and press **Enter**.

Result: CSUtil.exe exports information for all users in the CiscoSecure user database to a file named `users.txt`.

Step 4 To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

Downloaded from www.Manualslib.com manuals search engine

Exporting Group Information to a Text File

You can use the -g option to export group configuration data, including device command sets, from the CiscoSecure user database to a text file named `groups.txt`. The `groups.txt` file is useful primarily for debugging purposes while working with the TAC.

Note Using the -g option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To export group information from the CiscoSecure user database to a text file, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 2 If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

Result: The CSAuth service stops.

Step 3 Type:

```
CSUtil.exe -g
```

and press **Enter**.

Result: CSUtil.exe exports information for all groups in the CiscoSecure user database to a file named `groups.txt`.

Step 4 To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

Downloaded from www.Manualslib.com manuals search engine

Exporting Registry Information to a Text File

You can use the -y option to export Windows Registry information for Cisco Secure ACS. CSUtil.exe exports the Registry information to a file named `setup.txt`. The `setup.txt` file is primarily useful for debugging purposes while working with the TAC.

To export registry information from Cisco Secure ACS to a text file, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 2 Type:

```
CSUtil.exe -y
```

and press **Enter**.

Result: CSUtil.exe exports Windows Registry information for Cisco Secure ACS to a file named `setup.txt`.

Decoding Error Numbers

You can use the -e option to decode error numbers found in Cisco Secure ACS service logs. These are error codes internal to Cisco Secure ACS. For example, the CSRadius log could contain a message similar to the following:

```
CSRadius/Logs/RDS.log:RDS 05/22/2001 10:09:02 E 2152 4756 Error -1087
authenticating geddy - no NAS response sent
```

In this example, the error code number that you could use CSUtil.exe to decode is "-1087":

```
C:\Program Files\CiscoSecure ACS vx.x\Utils: CSUtil.exe -e -1087
CSUtil v3.0(1.14), Copyright 1997-2001, Cisco Systems Inc
Code -1087 : External database reported error during authentication
```


Downloaded from www.Manualslib.com manuals search engine

Note The -e option applies to Cisco Secure ACS internal error codes only, not to Windows error codes sometimes captured in Cisco Secure ACS logs, such as when Windows NT/2000 authentication fails.

For more information about Cisco Secure ACS service logs, see the "Service Logs" section on page 9-34.

To decode an error number from a Cisco Secure ACS service log, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 2 Type:

```
CSUtil.exe -e -number
```

where *number* is the error number found in the Cisco Secure ACS service log. Press **Enter**.

Note The hyphen (-) before *number* is required.

Result: CSUtil.exe displays the text message equivalent to the error number specified.

Recalculating CRC Values

The -c option is for use by the TAC. Its purpose is to resolve CRC (cyclical redundancy check) value conflicts between files manually copied into your Cisco Secure ACS directories and the values recorded in the Windows Registry.

Note Do not use the -c option unless a Cisco representative requests that you do.

Downloaded from www.Manualslib.com manuals search engine

User-Defined RADIUS Vendors and VSA Sets

This section provides information and procedures about user-defined RADIUS vendors and VSAs. It contains the following topics:

- About User-Defined RADIUS Vendors and VSA Sets, page E-27
- Adding a Custom RADIUS Vendor and VSA Set, page E-28
- Deleting a Custom RADIUS Vendor and VSA Set, page E-29
- Listing Custom RADIUS Vendors, page E-30
- RADIUS Vendor/VSA Import File, page E-31

About User-Defined RADIUS Vendors and VSA Sets

In addition to a set of predefined RADIUS vendors and vendor-specific attributes (VSAs), Cisco Secure ACS supports RADIUS vendors and VSAs that you define. CSUtil.exe provides the mechanism for adding and deleting your custom RADIUS vendors and VSAs. Vendors you add must be IETF-compliant; therefore, all VSAs that you add must be sub-attributes of IETF RADIUS attribute number 26.

You can define up to ten custom RADIUS vendors, numbered 0 (zero) through 9. CSUtil.exe allows only one instance of any given vendor, as defined by the vendor's unique IETF ID number and by the vendor name.

Note If you intend to replicate user-defined RADIUS vendor and VSA configurations, user-defined RADIUS vendor and VSA definitions to be replicated must be identical on the primary and secondary Cisco Secure ACS servers, including the RADIUS vendor slots that the user-defined RADIUS vendors occupy. For more information about database replication, see the "CiscoSecure Database Replication" section on page 8-6.

Downloaded from www.Manualslib.com manuals search engine

Adding a Custom RADIUS Vendor and VSA Set

You can use the -addUDV option to add up to ten custom RADIUS vendors and VSA sets to Cisco Secure ACS. Each RADIUS vendor and VSA set is added to one of ten possible user-defined RADIUS vendor slots.

Note While CSUtil.exe adds a custom RADIUS vendor and VSA set to Cisco Secure ACS, all Cisco Secure ACS services are automatically stopped and restarted. No users are authenticated while this process is occurring.

Before You Begin

- Define a custom RADIUS vendor and VSA set in a RADIUS vendor/VSA import file. For more information, see the .
- Determine the RADIUS vendor slot to which you want to add the new RADIUS vendor and VSAs. For more information, see the "Listing Custom RADIUS Vendors" section on page E-30.

To add a custom RADIUS VSA to Cisco Secure ACS, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 2 Type:

```
CSUtil.exe -addUDV  slot-number filename
```

where *slot-number* is an unused Cisco Secure ACS RADIUS vendor slot and *filename* is the name of a RADIUS vendor/VSA import file. *filename* can include a relative or absolute path to the RADIUS vendor/VSA import file. Press **Enter**.

For example, to add the RADIUS vendor defined in `d:\acs\myvsa.ini` to slot 5, the command would be:

```
CSUtil.exe -addUDV 5 d:\acs\myvsa.ini
```

Result: CSUtil.exe displays a confirmation prompt.

Downloaded from www.Manualslib.com manuals search engine

Step 3 To confirm that you want to add the RADIUS vendor and halt all Cisco Secure ACS services during the process, type **Y** and press **Enter**.

Result: CSUtil.exe halts Cisco Secure ACS services, parses the vendor/VSA input file, and adds the new RADIUS vendor and VSAs to Cisco Secure ACS. This process may take a few minutes. After it is complete, CSUtil.exe restarts Cisco Secure ACS services.

Note We recommend that you archive RADIUS vendor/VSA import files. During upgrades, the Utils directory, where CSUtil.exe is located, is replaced, including all its contents. Backing up RADIUS vendor/VSA import files ensures that you can recover your custom RADIUS vendors and VSAs after reinstallation or upgrading to a later release.

Deleting a Custom RADIUS Vendor and VSA Set

You can use the -delUDV option to delete a custom RADIUS vendor from Cisco Secure ACS.

Note While CSUtil.exe deletes a custom RADIUS vendor from Cisco Secure ACS, all Cisco Secure ACS services are automatically stopped and restarted. No users are authenticated while this process is occurring.

Before You Begin

Verify that, in the Network Configuration section of the Cisco Secure ACS HTML interface, no AAA client uses the RADIUS vendor. For more information about configuring AAA clients, see the "AAA Client Configuration" section on page 4-8.

Verify that your RADIUS accounting log does not contain attributes from the RADIUS vendor you want to delete. For more information about configuring your RADIUS accounting log, see the "RADIUS Accounting Log" section on page 9-7.

Downloaded from www.Manualslib.com manuals search engine

To delete a custom RADIUS vendor and VSA set from Cisco Secure ACS, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 2 Type:

```
CSUtil.exe -delUDV  slot-number
```

where *slot-number* is the slot containing the RADIUS vendor that you want to delete. Press **Enter**.

Note For more information about determining what RADIUS vendor a particular slot contains, see the "Listing Custom RADIUS Vendors" section on page E-30.

Result: CSUtil.exe displays a confirmation prompt.

Step 3 To confirm that you want to halt all Cisco Secure ACS services while deleting the custom RADIUS vendor and VSAs, type **Y** and press **Enter**.

Result: CSUtil.exe displays a second confirmation prompt.

Step 4 To confirm that you want to delete the RADIUS vendor, type **Y** and press **Enter**.

Result: CSUtil.exe halts Cisco Secure ACS services, deletes the specified RADIUS vendor from Cisco Secure ACS. This process may take a few minutes. After it is complete, CSUtil.exe restarts Cisco Secure ACS services.

Listing Custom RADIUS Vendors

You can use the -listUDV option to determine what custom RADIUS vendors are defined in Cisco Secure ACS. This option also enables you to determine which of the ten possible custom RADIUS vendor slots are in use and which RADIUS vendor occupies each used slot.

Downloaded from www.Manualslib.com manuals search engine

To list all custom RADIUS vendors defined in Cisco Secure ACS, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "Location of CSUtil.exe and Related Files" section on page E-2.

Step 2 Type:

```
CSUtil.exe -listUDV
```

Press **Enter**.

Result: CSUtil.exe lists each user-defined RADIUS vendor slot in slot number order. CSUtil.exe lists slots that do not contain a custom RADIUS vendor as "Unassigned". An unassigned slot is empty. You can add a custom RADIUS vendor to any slot listed as "Unassigned".

RADIUS Vendor/VSA Import File

To import a custom RADIUS vendor and VSA set into Cisco Secure ACS, you must define the RADIUS vendor and VSA set in an import file.

We recommend that you archive RADIUS vendor/VSA import files. During upgrades, the `Utils` directory, where CSUtil.exe is located, is replaced, including all its contents. Backing up RADIUS vendor/VSA import files ensures that you can recover your custom RADIUS vendors and VSAs after reinstallation or upgrading to a later release.

This section details the format and content of RADIUS VSA import files. It includes the following topics:

- About the RADIUS Vendor/VSA Import File, page E-32
- Vendor and VSA Set Definition, page E-33
- Attribute Definition, page E-34
- Enumeration Definition, page E-35
- Example RADIUS Vendor/VSA Import File, page E-37

Downloaded from www.Manualslib.com manuals search engine

About the RADIUS Vendor/VSA Import File

RADIUS Vendor/VSA import files use a Windows .ini file format. Each RADIUS vendor/VSA import file comprises three types of sections, detailed in Table E-7. Each section comprises a section header and a set of keys and values. The order of the sections in the RADIUS vendor/VSA import file is irrelevant.

Table E-7 RADIUS VSA Import File Section Types

Section	Required	Number	Description
Vendor and VSA set definition	Yes	1	Defines the RADIUS vendor and VSA set. For more information, see the "Vendor and VSA Set Definition" section on page E-33.
Attribute definition	Yes	1 to 255	Defines a single attribute of the VSA set. For more information, see the "Attribute Definition" section on page E-34.
Enumeration	No	0 to 255	Defines enumerations for attributes with integer data types. For more information, see the "Enumeration Definition" section on page E-35.

Downloaded from www.Manualslib.com manuals search engine

Vendor and VSA Set Definition

Each RADIUS vendor/VSA import file must have one vendor and VSA set section. The section header must be "[User Defined Vendor]". Table E-8 lists valid keys for the vendor and VSA set section.

Table E-8 Vendor and VSA Set Keys

Keys	Required	Value Required	Description
Name	Yes	Vendor name	The name of the RADIUS vendor.
IETF Code	Yes	An integer	The IETF-assigned vendor number for this vendor.
VSA *n* (where *n* is the VSA number)	Yes—you can define 1 to 255 VSAs	Attribute name	The name of a VSA. For each VSA named here, the file must contain a corresponding attribute definition section. Attribute names must be unique within the RADIUS vendor/VSA import file, and within the set of all RADIUS attributes in Cisco Secure ACS. To facilitate this, we recommend that you prefix the vendor name to each attribute name, such as "widget-encryption" for an encryption-related attribute for the vendor Widget. This also makes accounting logs easier to understand.

For example, the following vendor and VSA set section defines the vendor "Widget", whose IETF-assigned vendor number is 9999. Vendor Widget has 4 VSAs (thus requiring 4 attribute definition sections):

```
[User Defined Vendor]
Name=Widget
IETF Code=9999
VSA 1=widget-encryption
VSA 2=widget-admin-interface
VSA 3=widget-group
VSA 4=widget-admin-encryption
```


Downloaded from www.Manualslib.com manuals search engine

Attribute Definition

Each RADIUS vendor/VSA import file must have one attribute definition section for each attribute defined in the vendor and VSA set section. The section header of each attribute definition section must match the attribute name defined for that attribute in the vendor and VSA set section. Table E-9 lists the valid keys for an attribute definition section.

Table E-9 Attribute Definition Keys

Keys	Required	Value Required	Description
Type	Yes	See Description.	The data type of the attribute. It must be one of the following: STRING INTEGER IPADDR If the attribute is an integer, the Enums key is valid.

Profile	Yes	See Description.	The attribute profile defines if the attribute is used for authorization or accounting (or both). At least one of the following two values must be present in the Profile key definition:
			IN—The attribute is used for accounting. After you add the attribute to Cisco Secure ACS, you can configure your RADIUS accounting log to record the new attribute. For more information about RADIUS accounting logs, see the "RADIUS Accounting Log" section on page 9-7.
			OUT—The attribute is used for authorization.
			In addition, you can use the value "MULTI" to allow several instances of the attribute per RADIUS message.
			Combinations are valid. For example:
			`Profile=MULTI OUT`
			or
			`Profile=IN OUT`

Downloaded from www.Manualslib.com manuals search engine

Table E-9 Attribute Definition Keys (continued)

Keys	Required	Value Required	Description
Enums	No (only valid when the TYPE value is INTEGER)	Enumerations section name	The name of the enumeration section. Several attributes can reference the same enumeration section. For more information, see the "Enumeration Definition" section on page E-35.

For example, the following attribute definition section defines the widget-encryption VSA, which is an integer used for authorization, and for which enumerations exist in the Encryption-Types enumeration section:

```
[widget-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types
```

Enumeration Definition

Enumeration definitions enable you to associate a text-based name for each valid numeric value of an integer-type attribute. In the Group Setup and User Setup sections of the Cisco Secure ACS HTML interface, the text values you define appear in lists associated with the attributes that use the enumerations. Enumeration definition sections are required only if an attribute definition section references them. Only attributes that are integer-type attributes can reference an enumeration definition section.

The section header of each enumeration definition section must match the value of an Enums key that references it. An enumeration definition section can be referenced by more than one Enums key, thus allowing for reuse of common enumeration definitions. An enumeration definition section can have up to 1000 keys.

Table E-10 on page E-36 lists the valid keys for an enumeration definition section.

Downloaded from www.Manualslib.com manuals search engine

Table E-10 Enumerations Definition Keys

Keys	Required	Value Required	Description
n (See Description.)	Yes	String	For each valid integer value of the corresponding attribute, an enumerations section must have one key. Each key defines a string value associated with an integer value. Cisco Secure ACS uses these string values in the HTML interface. For example, if 0 through 4 are valid integer values for a given attribute, its enumeration definition would contain the following: 0=*value0* 1=*value1* 2=*value2* 3=*value3* 4=*value4*

For example, the following enumerations definition section defines the Encryption-Types enumeration, which associates the string value 56-bit with the integer 0 and the string value 128-bit with the integer 1:

```
[Encryption-Types]
0=56-bit
1=128-bit
```


Downloaded from www.Manualslib.com manuals search engine

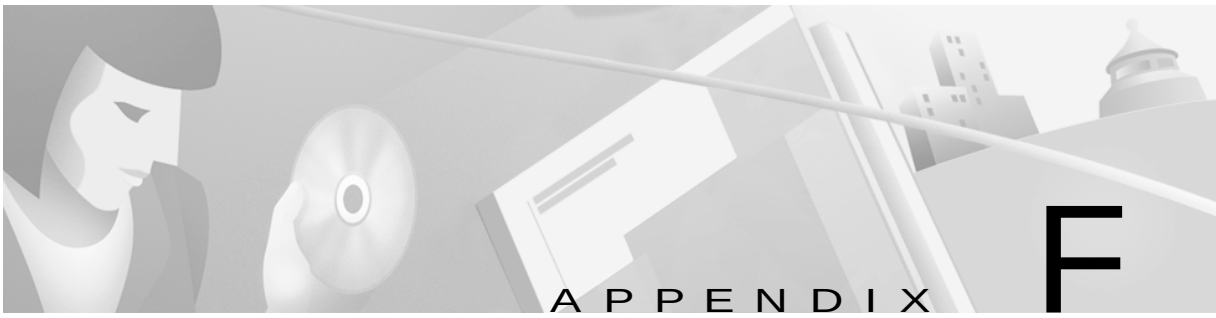
Example RADIUS Vendor/VSA Import File

The example RADIUS vendor/VSA import file, below, defines the vendor Widget, whose IETF number is 9999. The vendor Widget has 5 VSAs. Of those attributes, 4 are for authorization and one is for accounting. Only one attribute can have multiple instances in a single RADIUS message. Two attributes have enumerations for their valid integer values and they share the same enumeration definition section.

```
[User Defined Vendor]
Name=Widget
IETF Code=9999
VSA 1=widget-encryption
VSA 2=widget-admin-interface
VSA 3=widget-group
VSA 4=widget-admin-encryption
VSA 5=widget-remote-address

[widget-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types

[widget-admin-interface]
Type=IPADDR
Profile=OUT

[widget-group]
Type=STRING
Profile=MULTI OUT

[widget-admin-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types

[widget-remote-address]
Type=STRING
Profile=IN

[Encryption-Types]
0=56-bit
1=128-bit
2=256-bit
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine



Cisco Secure ACS and Virtual Private Dial-up Networks

Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) supports authentication forwarding of virtual private dial-up network (VPDN) requests. There are two basic types of "roaming" users: Internet and intranet; VPDN addresses the requirements of roaming intranet users. This chapter provides information about the VPDN process and how it affects the operation of Cisco Secure ACS.

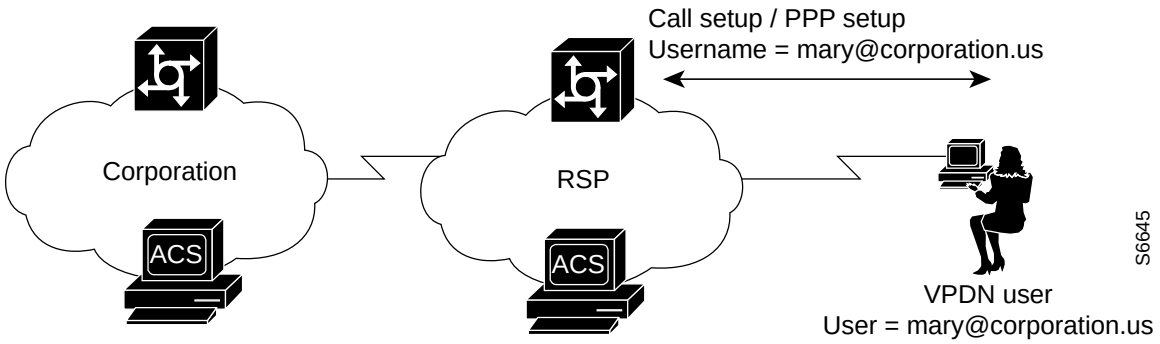
VPDN Process

This section describes the steps for processing VPDN requests in a standard environment.

1. A VPDN user dials in to the network access server (NAS) of the regional service provider (RSP). The standard call/point-to-point protocol (PPP) setup is done. A username and password are sent to the NAS in the format username@domain (for example, mary@corporation.us). See Figure F-1.

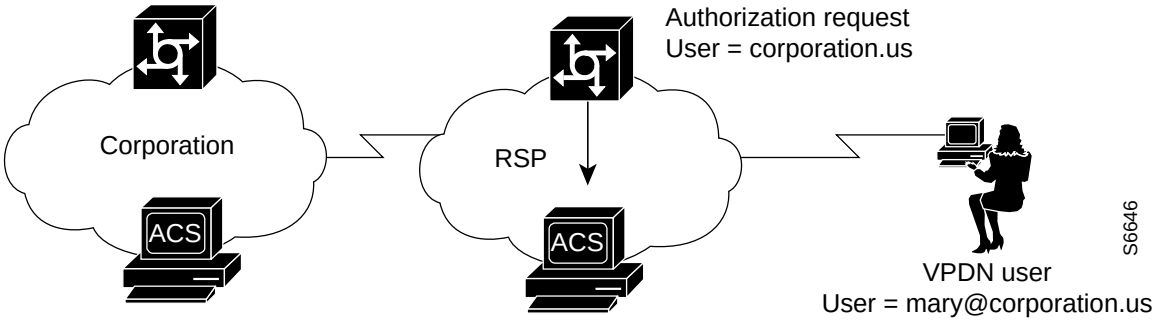
Downloaded from www.Manualslib.com manuals search engine

Figure F-1 VPDN User Dials In



2. If VPDN is enabled, the NAS assumes that the user is a VPDN user. The NAS strips off the "username@" (mary@) portion of the username and authorizes (not authenticates) the domain portion (corporation.us) with the ACS. See Figure F-2.

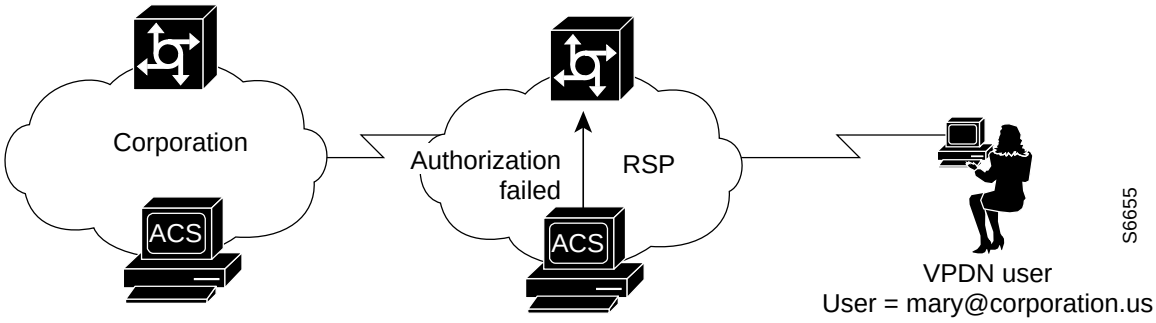
Figure F-2 NAS Attempts to Authorize Domain



3. If the domain authorization fails, the NAS assumes the user is not a VPDN user. The NAS then authenticates (not authorizes) the user as if the user is a standard non-VPDN dial user. See Figure F-3.

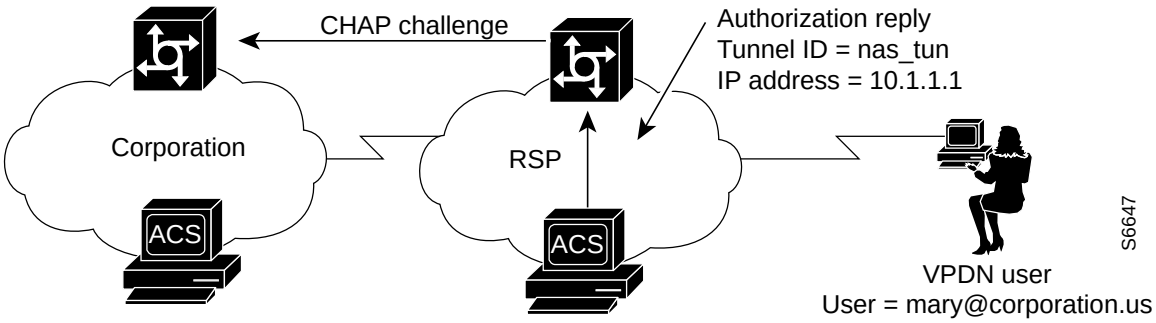
Downloaded from www.Manualslib.com manuals search engine

Figure F-3 Authorization of Domain Fails



If the ACS authorizes the domain, it returns the Tunnel ID and the IP address of the home gateway (HG); these are used to create the tunnel. See Figure F-4.

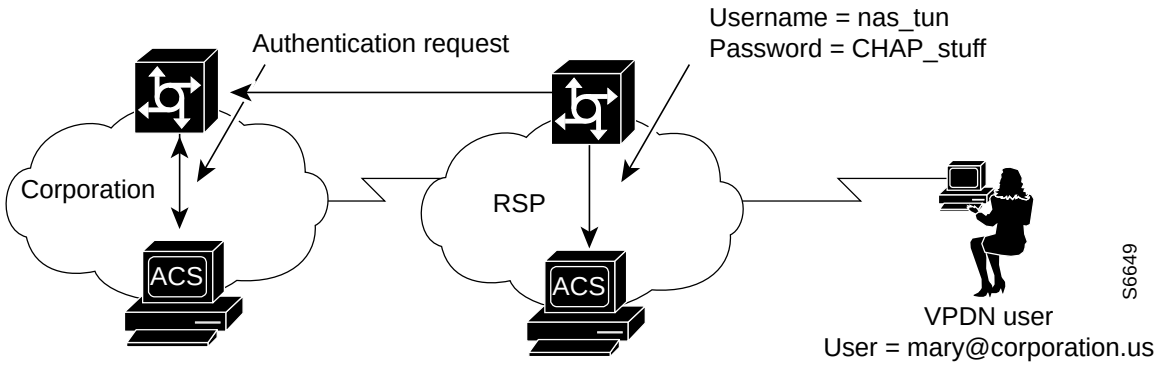
Figure F-4 ACS Authorizes Domain



4. The HG uses its ACS to authenticate the tunnel, where the username is the name of the tunnel (nas_tun). See Figure F-5 on page F-4.

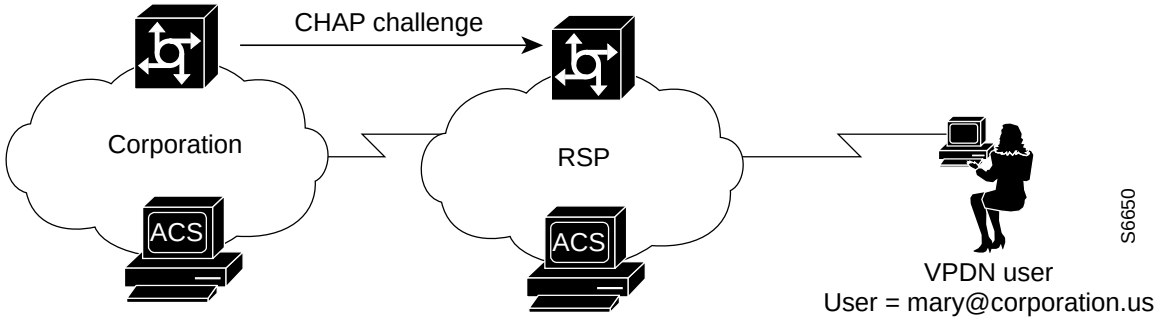
Downloaded from www.Manualslib.com manuals search engine

Figure F-5 HG Authenticates Tunnel with ACS



5. The HG now authenticates the tunnel with the NAS, where the username is the name of the HG. This name is chosen based on the name of the tunnel, so the HG might have different names depending on the tunnel being set up. See Figure F-6.

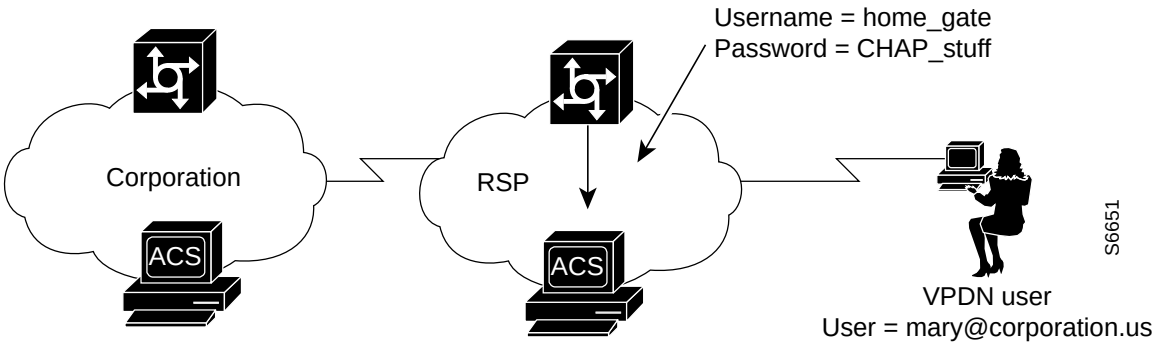
Figure F-6 HG Authenticates Tunnel with the NAS



6. The NAS now uses its ACS to authenticate the tunnel from the HG. See Figure F-7 on page F-5.

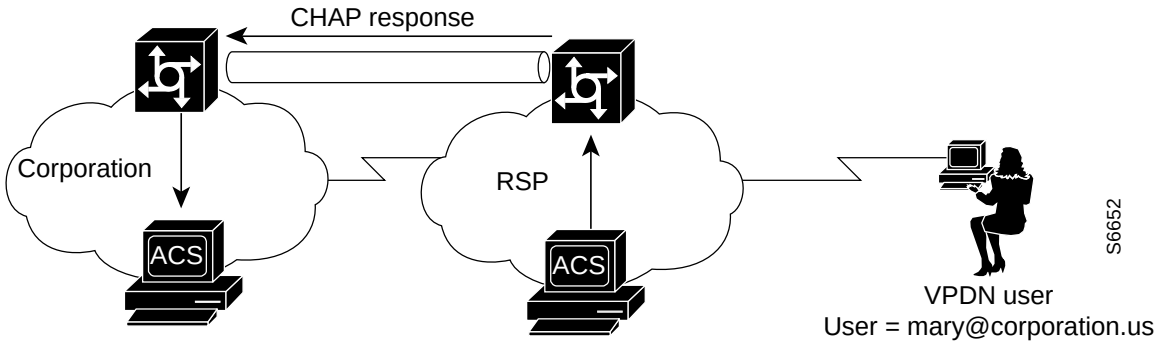
Downloaded from www.Manualslib.com manuals search engine

Figure F-7 NAS Authenticates Tunnel with ACS



7. After authenticating, the tunnel is established. Now the actual user (mary@corporation.us) must be authenticated. See Figure F-8.

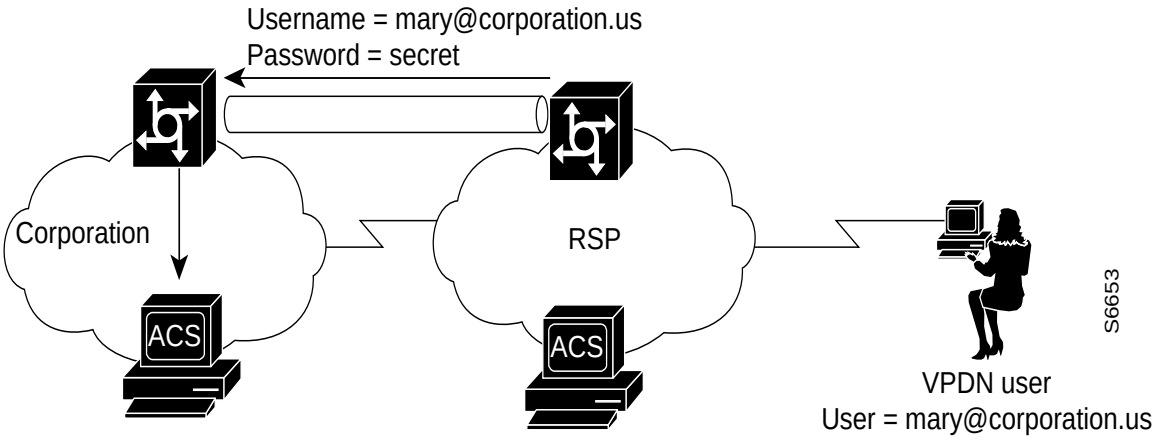
Figure F-8 VPDN Tunnel is Established



8. The HG now authenticates the user as if the user dialed directly in to the HG. The HG might now challenge the user for a password. The Cisco Secure ACS at RSP can be configured to strip off the @ and domain before it passes the authentication to the HG. (The user is passed as mary@corporation.us.) The HG uses its ACS to authenticate the user. See Figure F-9 on page F-6.

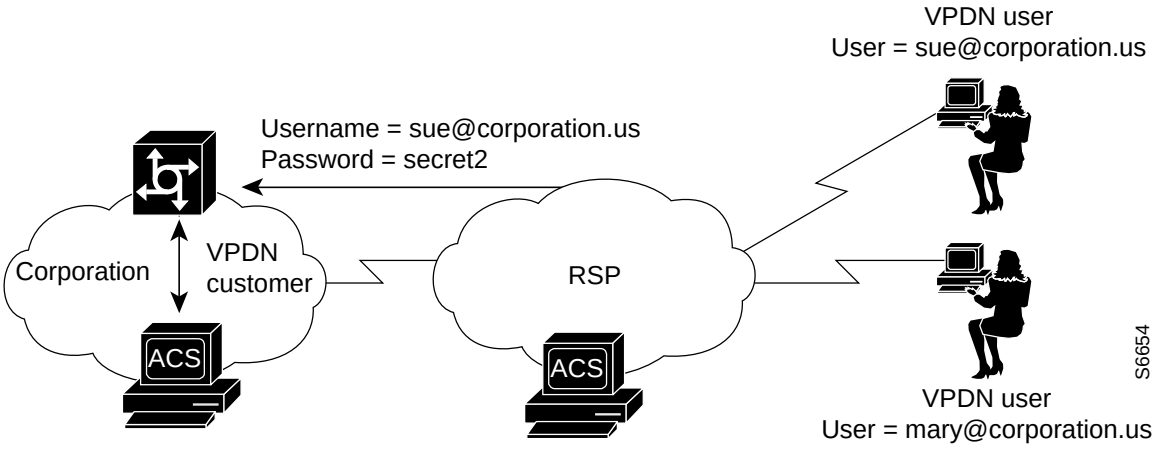
Downloaded from www.Manualslib.com manuals search engine

Figure F-9 HG Uses ACS to Authenticate User

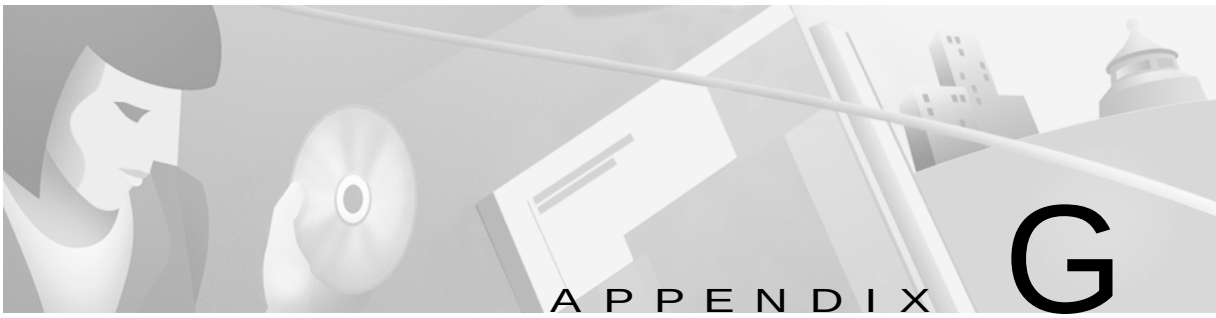


9. If another user (sue@corporation.us) dials in to the NAS while the tunnel is up, the NAS does not repeat the entire authorization/authentication process. Instead, it passes the user through the existing tunnel to the HG. See Figure F-10.

Figure F-10 Another User Dials In While Tunnel is Up



Downloaded from www.Manualslib.com manuals search engine



ODBC Import Definitions

ODBC import definitions are a listing of the action codes allowable in an accountActions table. The RDBMS Synchronization feature of Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) uses a table named “accountActions” as input for automated or manual updates of the CiscoSecure user database. For more information about the RDBMS Synchronization feature and the accountActions table, see the “RDBMS Synchronization” section on page 8-24.

This appendix contains the following sections:

- accountActions Table Specification, page G-1
- Action Codes, page G-5
- Cisco Secure ACS Attributes and Action Codes, page G-31
- An Example accountActions Table, page G-36

accountActions Table Specification

The third-party system that writes to the accountActions table must adhere to the accountActions table specification and must only use the action codes detailed in the “Action Codes” section on page G-5. Otherwise, RDBMS Synchronization may import incorrect information into the CiscoSecure user database or may fail to occur at all.

Downloaded from www.Manualslib.com manuals search engine

accountActions Table Format

Each row in an accountActions table has 14 fields (or columns). Table G-1 on page G-2 lists the fields that compose an accountActions table in the order in which they appear in the table.

The one-letter or two-letter abbreviations given in the Mnemonic column are a shorthand notation used to indicate required fields for each action code in the "Action Codes" section on page G-5.

To see an accountActions table, see the "An Example accountActions Table" section on page G-36.

Table G-1 accountActions Table

Field Name	Mnemonic	Type	Size	Comments
SequenceId	SI	AutoNumber	32	The unique action ID.
Priority	P	Int	—	The priority with which this update is to be treated. 0 is the lowest priority.
UserName	UN	String	32	The name of the user to which the transaction applies.
GroupName	GN	String	32	The name of a group to which the transaction applies.
Action	A	Number	0-2^16	The Action required. (See the "Action Codes" section on page G-5.)
ValueName	VN	String	255	The name of the parameter to change.
Value1	V1	String	255	The new value (for numeric parameters, this is a decimal string).
Value2	V2	String	255	The name of a TACACS+ protocol; for example, "ip" or RADIUS VSA Vendor ID.

Downloaded from www.Manualslib.com manuals search engine

Table G-1 accountActions Table (continued)

Field Name	Mnemonic	Type	Size	Comments
Value3	V3	String	255	The name of a TACACS+ service; for example, "ppp" or the RADIUS VSA attribute number.
DateTime	DT	DateTime	—	The date/time the Action was created.
MessageNo	MN	Int	—	Used to number related transactions for audit purposes.
ComputerNames	CN	String	32	RESERVED by CSDBSync.
AppId	AI	String	255	The type of configuration parameter to change.
Status	S	Number	32	TRI-STATE:0=not processed, 1=done, 2=failed. This should normally be set to 0.

accountActions Table Mandatory Fields

Three fields in the accountActions table are required for every type of transaction. The tables in the following sections specify which fields must be present for each transaction type or action.

The following three fields are required for all transaction types:

- Action
- DateTime
- SequenceID

Downloaded from www.Manualslib.com manuals search engine

In addition to the three required fields above, the UserName and GroupName fields are required for many actions:

- If a transaction is acting upon a user account, a value is required in the UserName field.
- If a transaction is acting upon a group, a value is required in the GroupName field.
- If a transaction is acting upon AAA client configuration, neither the UserName field nor the GroupName field is required.

Note The UserName and GroupName fields are mutually exclusive; only one of these two fields can have a value and neither field is always required.

accountActions Table Processing Order

Cisco Secure ACS reads rows from the accountActions table and processes them in a specific order. Cisco Secure ACS determines the order first by the values in the Priority fields (mnemonic: P) and then by the values in the Sequence ID fields (mnemonic: SI). Cisco Secure ACS processes the rows with the highest priority first. If rows have an equal priority, Cisco Secure ACS processes them by their sequence ID, with the lowest sequence ID processed first. For example, if the priority for row A is higher than the priority for row B, Cisco Secure ACS would process row A first, regardless of whether row B has a lower sequence ID or not.

Thus, the Priority field (P) enables transactions of higher importance to occur first, such as deleting a user or changing a password. In the most common implementations of RDBMS Synchronization, the third-party system writes to the accountActions table in batch mode, with all actions (rows) assigned a priority of zero (0).

Note When changing transaction priorities, be careful that they are processed in the correct order; for example, a user account must be created before the user password is assigned.

Downloaded from www.Manualslib.com manuals search engine

You can use the MessageNo field (mnemonic: MN) to associate related transactions, such as the addition of a user and subsequent actions to set password values and status. You can use the MessageNo field to create an audit trail for the third-party system that writes to the accountActions table.

Action Codes

This section provides the action codes valid for use in the Action field (mnemonic: A) of your accountActions table. The Required column uses the field mnemonic names to indicate which fields should be completed, except for the mandatory fields, which are assumed. For more information about the mnemonic names of accountActions table fields, see Table G-1 on page G-2. For more information about the mandatory fields, see the "accountActions Table Mandatory Fields" section on page G-3.

If an action can be applied to either a user or group, "UN|GN" appears, using the vertical bar to indicate that either one of the two fields is required. To make the action affect only the user, leave the group name empty, and vice versa.

This section contains the following topics about action codes:

- Action Codes for Setting and Deleting Values, page G-5
- Action Codes for Creating and Modifying User Accounts, page G-7
- Action Codes for Initializing and Modifying Access Filters, page G-15
- Action Codes for Modifying TACACS+ and RADIUS Group and User Settings, page G-20
- Action Codes for Modifying Network Configuration, page G-27
- Action Code for Deleting the CiscoSecure User Database, page G-31

Action Codes for Setting and Deleting Values

The two most fundamental action codes are SET_VALUE (action code: 1) and DELETE_VALUE (action code: 2), described in Table G-2 on page G-6.

The SET_VALUE (action code: 1) and DELETE_VALUE (action code: 2) actions, described in Table G-2 on page G-6, instruct RDBMS Synchronization to assign a value to various internal attributes in Cisco Secure ACS. Unless asked to

Downloaded from www.Manualslib.com manuals search engine

use these action codes for other purposes by a Cisco representative, you can only use these action codes for assigning values to user-defined fields (see the "User-Specific Attributes" section on page G-31).

Table G-2 Action Codes for Setting and Deleting Values

Action Code	Name	Required	Description

1	SET_VALUE	UN|GN, AI, VN, V1, V2	Sets a value (V1) named (VN) of type (V2) for app (AI).
			App IDs (AI) can be one of the following:
			• APP_CSAUTH
			• APP_CSTACACS
			• APP_CSRADIUS
			• APP_CSADMIN
			Value types (V2) can be one of the following:
			• **TYPE_BYTE**—Single 8-bit number.
			• **TYPE_SHORT**—Single 16-bit number.
			• **TYPE_INT**—Single 32-bit number.
			• **TYPE_STRING**—Single string.
			• **TYPE_ENCRYPTED_STRING**—Single string to be saved encrypted.
			• **TYPE_MULTI_STRING**—Tab-separated set of substrings.
			• **TYPE_MULTI_INT**—Tab-separated set of 32-bit numbers.
			For example:
			`UN="fred"`
			`AI="APP_CSAUTH"`
			`VN="My Value"`
			`V2="TYPE_MULTI_STRING"`
			`V1="str1<tab>str2<tab>str3"`

Downloaded from www.Manualslib.com manuals search engine

Table G-2 Action Codes for Setting and Deleting Values (continued)

Action Code	Name	Required	Description
2	DELETE_ VALUE	UN|GN, AI, VN	Delete value (VN) for app (AI) and user (UN).

Action Codes for Creating and Modifying User Accounts

Table G-3 lists the action codes for creating, modifying, and deleting user accounts.

Note Before you can modify a user account, such as assigning a password, you must create the user account, either in the HTML interface or by using the ADD_USER action (action code: 100).

Transactions using these codes affect the configuration displayed in the User Setup section of the HTML interface. For more information about the User Setup section, see Chapter 7, "Setting Up and Managing User Accounts."

Table G-3 User Creation and Modification Action Codes

Action Code	Name	Required	Description
100	ADD_USER	UN, V1	Create a user (32 characters maximum). V1 is used as the initial password. Optionally, the user can also be assigned to a group.
101	DELETE_USER	UN	Remove a user.
102	SET_PAP_PASS	UN, V1	Set the PAP password for a user (64 ASCII characters maximum). CHAP/ARAP will also default to this.
103	SET_CHAP_PASS	UN, V1	Set the CHAP/ARAP password for a user (64 characters maximum).
104	SET_OUTBOUND_ CHAP_PASS	UN, V1	Sets the CHAP/ARAP password for a user (32 characters maximum).

Downloaded from www.Manualslib.com manuals search engine

Table G-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
105	SET_T+_ENABLE_ PASS	UN, V1, V2	Sets the TACACS+ enable password (V1) (32 characters maximum) and Max Privilege level (V2) (0-15).
106	SET_GROUP	UN, GN	Set the user's Cisco Secure ACS group assignment.

Downloaded from www.Manualslib.com manuals search engine

Table G-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
108	SET_PASS_TYPE	V1	Set the password type of the user. This can be one of the CiscoSecure user database password types or any of the external databases supported: • **PASS_TYPE_CSDB**—CSDB internal password • **PASS_ TYPE_CSDB_UNIX**—CSDB internal password (UNIX encrypted) • **PASS_TYPE_NT**—External Windows NT/2000 database password • **PASS_TYPE_NDS**—External Novell database password • **PASS_TYPE_LDAP**—External generic LDAP database password • **PASS_TYPE_SDI**—External RSA Security database password • **PASS_TYPE_ANPI**—External AXENT database password • **PASS_TYPE_ENIGMA**—External SafeWord database password • **PASS_TYPE_CRYPTO**—External CRYPTOCard database password • **PASS_TYPE_ODBC**—External ODBC database password • **PASS_TYPE_LEAP**—External LEAP proxy RADIUS server database password • **PASS_TYPE_ACTIVCARD**—External ActivCard database password • **PASS_TYPE_VASCO**—External Vasco database password • **PASS_TYPE_RADIUS_TOKEN**—External RADIUS token server database password

Downloaded from www.Manualslib.com manuals search engine

Table G-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
109	REMOVE_PASS_ STATUS	UN,V1	Remove a password status flag. This results in the status states being linked in a logical XOR condition by the CSAuth server. V1 should contain one of the following: • **PASS_STATUS_EXPIRES**—Password expires on a given date. • **PASS_STATUS_NEVER**—Password never expires. • **PASS_STATUS_WRONG**—Password expires after a given number of attempts. • **PASS_STATUS_DISABLED**—The account has been disabled.
110	ADD_PASS_STATUS	UN, V1	Defines how a password should be expired by Cisco Secure ACS. To set multiple password states for a user, use multiple instances of this action. This results in the status states being linked in a logical XOR condition by the CSAuth server. V1 should contain one of the following: • **PASS_STATUS_EXPIRES**—Password expires on a given date. • **PASS_STATUS_NEVER**—Password never expires. • **PASS_STATUS_WRONG**—Password expires after a given number of attempts. • **PASS_STATUS_RIGHT**—Password expires after a given number of attempts. • **PASS_STATUS_DISABLED**—The account has been disabled.
112	SET_PASS_EXPIRY _WRONG	UN,V1	Set the maximum number of bad authentications allowed (automatic reset on good password if not exceeded) and reset current count.

Downloaded from www.Manualslib.com manuals search engine

Table G-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
113	SET_PASS_EXPIRY_DATE	UN,V1	Set the date on which the account expires. The date format should be YYYYMMDD.
114	SET_MAX_SESSIONS	UN|GN,V1	• Set the maximum number of simultaneous sessions for a user or group. V1 should contain one of the following values: • MAX_SESSIONS_UNLIMITED • MAX_SESSIONS_AS_GROUP • 1-65534
115	SET_MAX_SESSIONS_GROUP_USER	GN,V1	Set the max sessions for a user of the group to one of the following values: • MAX_SESSIONS_UNLIMITED • 1-65534

Downloaded from www.Manualslib.com manuals search engine

Table G-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
260	SET_QUOTA	GN,VN,V1, V2	Used to set a quota for a user or group. VN defines the quota type. Valid values are: • **online time**—The quota limits the user or group by the number of seconds logged in to the network for the period defined in V2. • **sessions**—The quota limits the user or group by the number of sessions on the network for the period defined in V2. V1 defines the quota. If VN is set to sessions, V1 is the maximum number of sessions in the period defined in V2. If VN is set to online time, V1 is the maximum number of seconds. V2 holds the period for the quota. Valid values are: • **QUOTA_PERIOD_DAILY**—The quota is enforced in 24-hour cycles, from 12:01 A.M. to midnight. • **QUOTA_PERIOD_WEEKLY**—The quota is enforced in 7-day cycles, from 12:01 A.M. Sunday until midnight Saturday. • **QUOTA_PERIOD_MONTHLY**—The quota is enforced in monthly cycles, from 12:01 A.M. on the first of the month until midnight on the last day of the month. • **QUOTA_PERIOD_ABSOLUTE**—The quota is enforced in an ongoing basis, without an end.

Downloaded from www.Manualslib.com manuals search engine

Table G-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
261	DISABLE_QUOTA	UN|GN,VN	Disable a group or user usage quota. VN defines the quota type. Valid values are: • **online time**—The quota limits the user or group by the number of seconds logged in to the network for the period defined in V2. • **sessions**—The quota limits the user or group by the number of sessions on the network for the period defined in V2.
262	SET_QUOTA_ APPLY_TYPE	UN,VN	Defines whether a user's usage quota is determined by the user's group quota or by a quota unique to the user. V1 makes this specification. Valid values for V1 are: • ASSIGNMENT_FROM_USER • ASSIGNMENT_FROM_GROUP
263	RESET_COUNTERS	UN|GN	Resets usage quota counters for a user or group.

Downloaded from www.Manualslib.com manuals search engine

Table G-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
270	SET_DCS_TYPE	UN|GN,VN, V1, Optionally V2	Set the type of device command set (DCS) authorization for a group or user. VN defines the service. Valid service types are: **shell**—Cisco IOS shell command authorization. **pixshell**—Cisco PIX command authorization. If additional DCS types have been added to your Cisco Secure ACS, you can find the valid value in the Interface Configuration page for TACACS+ (Cisco IOS). The valid values appear in parentheses after the service title, such as `PIX Shell (pixshell)`. V1 defines the assignment type. The valid values for VN are: **none**—Sets no DCS for the user or group. **as group**—For users only, this value signifies that the user's DCS settings for the service specified should be the same as the user's group DCS settings. **static**—Sets a DCS for the user or group for all devices enabled to perform command authorization for the service specified. If V1 is set to static, V2 is required and must contain the name of the DCS to assign to the user or group for the given service. **ndg**—Specifies that command authorization for the user or group is to be done on a per-NDG basis. Use action 271 to add DCS to NDG mappings for the user or group. Changing a user or group assignment type (V1) results in clearing previous data, including NDG to DCS mappings (defined by action 271).

Downloaded from www.Manualslib.com manuals search engine

Table G-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
271	SET_DCS_NDG_MAP	UN|GN,VN, V1,V2	When the assignment type specified by a 270 action code is ndg, use this action code to map between the device command set and the NDG. VN defines the service. Valid service types are: • **shell**—Cisco IOS shell command authorization. • **pixshell**—Cisco PIX command authorization. If additional DCS types have been added to your Cisco Secure ACS, you can find the valid value in the Interface Configuration page for TACACS+ (Cisco IOS). The valid values appear in parentheses after the service title, such as `PIX Shell (pixshell)`. V1 defines the name of the NDG. Use the name of the NDG as it appears in the HTML interface. For example, if you have configured an NDG named "East Coast NASes" and want to use action 271 to apply a DCS to that NDG, V1 should be "East Coast NASes". V2 defines the name of the DCS. Use the name of the DCS as it appears in the HTML interface. For example, if you have configured a DCS named "Tier2 PIX Admin DCS" and want to use action 271 to apply it to an NDG, V2 should be "Tier2 PIX Admin DCS".

Action Codes for Initializing and Modifying Access Filters

Table G-4 on page G-16 lists the action codes for initializing and modifying AAA client access filters. AAA client access filters control Telnet access to a AAA client. Dial access filters control access by dial-up users.

Transactions using these codes affect the configuration displayed in the User Setup and Group Setup sections of the HTML interface. For more information about the User Setup section, see Chapter 7, “Setting Up and Managing User Accounts.” For more information about the Group Setup section, see Chapter 6, “Setting Up and Managing User Groups.”

Downloaded from www.Manualslib.com manuals search engine

Table G-4 Action Codes for Initializing and Modifying Access Filters

Action Code	Name	Required	Description
120	INIT_NAS_ACCESS_ CONTROL	UN|GN,V1	Clear the AAA client access filter list and initialize permit/deny for any forthcoming filters. V1 should be one of the following values: • ACCESS_PERMIT • ACCESS DENY
121	INIT_DIAL_ACCESS_ CONTROL	UN|GN,V1	Clear the dial-up access filter list and initialize permit/deny for any forthcoming filters. V1 should be one of the following values: • ACCESS_PERMIT • ACCESS DENY
122	ADD_NAS_ACCESS_FILTER	UN|GN,V1	Add a AAA client filter for the user|group. V1 should contain a single (AAA client name, AAA client port, remote address, CLID) tuple; for example: `NAS01,tty0,0898-69696969` Optionally, the AAA client name can be "All AAA clients" to specify that the filter applies to all configured AAA clients and an asterisk (*) to represent all ports.

Downloaded from www.Manualslib.com manuals search engine

Table G-4 Action Codes for Initializing and Modifying Access Filters (continued)

Action Code	Name	Required	Description
123	ADD_DIAL_ACCESS_FILTER	UN|GN, V1, V2	Add a dial-up filter for the user|group. V1 should contain one of the following values: • Calling station ID • Called station ID • Calling and called station ID; for example: • 01732-875374,0898-69696969 AAA client IP address, AAA client port; for example: `10.45.6.123,tty0` V2 should contain the filter type as one of the following values: • **CLID**—The user is filtered by the calling station ID. • **DNIS**—The user is filtered by the called station ID. • **CLID/DNIS**—The user is filtered by both calling and called station IDs. • **AAA client/PORT**—The user is filtered by AAA client IP and AAA client port address.
130	SET_TOKEN_CACHE_ SESSION	GN, V1	Enable/disable token caching for an entire session; V1 is 0=disable, 1=enable.
131	SET_TOKEN_CACHE_TIME	GN, V1	Set the duration that tokens are cached. V1 is the token cache duration in seconds.

Downloaded from www.Manualslib.com manuals search engine

Table G-4 Action Codes for Initializing and Modifying Access Filters (continued)

Action Code	Name	Required	Description
140	SET_TODDOW_ACCESS	UN|GN, V1	Set periods during which access is permitted. V1 contains a string of 168 characters. Each character represents a single hour of the week. A "1" represents an hour that is permitted, while a "0" represents an hour that is denied. If this parameter is not specified for a user, the group setting applies. The default group setting is "111111111111" and so on.

Downloaded from www.Manualslib.com manuals search engine

Table G-4 Action Codes for Initializing and Modifying Access Filters (continued)

Action Code	Name	Required	Description
150	SET_STATIC_IP	UN, V1, V2	Configure the (TACACS+ and RADIUS) IP address assignment for this user. V1 holds the IP address in the following format: *xxx.xxx.xxx.xxx* V2 should be one of the following: • **ALLOC_METHOD_STATIC**—The IP address in V1 is assigned to the user in the format "xxx.xxx.xxx.xxx." • **ALLOC_METHOD_NAS_POOL**—The IP pool named in V1 (configured on the AAA client) will be assigned to the user. • **ALLOC_METHOD_AAA_POOL**—The IP pool named in V1 (configured on the AAA server) will be assigned to the user. • **ALLOC_METHOD_CLIENT**—The dial-in client will assign its own IP address. • **ALLOC_METHOD_AS_GROUP**—The IP address assignment configured for the group will be used.

Downloaded from www.Manualslib.com manuals search engine

Table G-4 Action Codes for Initializing and Modifying Access Filters (continued)

Action Code	Name	Required	Description
151	SET_CALLBACK_NO	UN|GN, V1	Set the callback number for this user or group (TACACS+ and RADIUS). V1 should be one of the following: **Callback number**—Literally, the phone number the AAA client is to call back. • **none**—No callback is allowed. • **roaming**—The dial-up client determines the callback number. • **as group**—Use the callback string or method defined by the group.

Action Codes for Modifying TACACS+ and RADIUS Group and User Settings

Table G-5 on page G-21 lists the action codes for creating, modifying, and deleting TACACS+ and RADIUS settings for Cisco Secure ACS groups and users. In the event that Cisco Secure ACS has conflicting user and group settings, user settings always override group settings.

Transactions using these codes affect the configuration displayed in the User Setup and Group Setup sections of the HTML interface. For more information about the User Setup section, see the "Setting Up and Managing User Accounts" section on page 7-1. For more information about the Group Setup section, see the "Setting Up and Managing User Groups" section on page 6-1.

Downloaded from www.Manualslib.com manuals search engine

Table G-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings

Action Code	Name	Required	Description

161	DEL_RADIUS_ ATTR	UN|GN, VN, Optionally V2, V3	Deletes the named RADIUS attribute for the group or user, where:
			• VN = “Vendor-Specific”
			• V2 = IETF vendor ID
			• V3 = VSA attribute ID
			For example, to specify the Cisco IOS/PIX vendor ID and the Cisco AV Pair:
			`VN=“Vendor-Specific”`
			`V2=“9”`
			`V3=“1”`

Downloaded from www.Manualslib.com manuals search engine

Table G-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description

163	ADD_RADIUS_ ATTR	UN|GN, VN, V1, Optionally V2, V3	Add the numbered attribute (VN) to value (V) for the user/group (UN|GN).
			For example:
			`GN="Group 1"`
			`VN="Reply Message"`
			`V1="Greetings"`
			`UN="fred"`
			`VN="Framed-IP-Address"`
			`V1="10.1.1.1"`
			When VN="Vendor-Specific", for the Vendor-Specific (VSA) attribute:
			• VN = "Vendor-Specific"
			• V2 = IETF vendor ID
			• V3 = VSA attribute ID
			For example:
			`V2="9"`
			`V3="1"`
			`V1="addr-pool=pool1"`
			RADIUS attribute values can be one of the following:
			• INTEGER
			• TIME
			• IP ADDRESS
			• STRING

Downloaded from www.Manualslib.com manuals search engine

Table G-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description

170	ADD_TACACS_ SERVICE	UN|GN, VN, V1, V3, Optionally V2	Permits the service for that user or group of users. For example:
			`GN="Group 1"`
			`V1="ppp"`
			`V2="ip"`
			or
			`UN="fred"`
			`V1="ppp"`
			`V2="ip"`
			or
			`UN="fred"`
			`V1=exec`

171	REMOVE_ TACACS_ SERVICE	UN|GN, V1
		Optionally V2
			Denies the service for that user or group of users. For example:
			`GN="Group 1", V1="ppp"`
			`V2="ip"`
			or
			`UN="fred"`
			`V1="ppp"`
			`V2="ip"`
			or
			`UN="fred"`
			`V1="exec"`
			This also resets the valid attributes for the service.

Downloaded from www.Manualslib.com manuals search engine

Table G-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description

172	ADD_TACACS_ ATTR	UN|GN, VN, V1, V3
		Optionally V2
			Sets a service specific attribute. The service must already have been permitted either via the HTML interface or using Action 170:
			`GN="Group 1"`
			`VN="routing"`
			`V1="ppp"`
			`V2="ip"`
			`V3="true"`
			or
			`UN="fred"`
			`VN="route"`
			`V1="ppp"`
			`V2="ip"`
			`V3=10.2.2.2`

173	REMOVE_ TACACS_ ATTR	UN|GN, VN, V1
		Optionally V2
			Removes a service-specific attribute:
			`GN="Group 1"`
			`V1="ppp"`
			`V2="ip"`
			`VN="routing"`
			or
			`UN="fred"`
			`V1="ppp"`
			`V2="ip"`
			`VN="route"`

Downloaded from www.Manualslib.com manuals search engine

Table G-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description

174	ADD_IOS_ COMMAND	UN|GN, VN, V1	Authorizes the given Cisco IOS command and determines if any arguments given to the command are to be found in a defined set or are not to be found in a defined set. The defined set is created using Actions 176 and 177:
			`GN="Group 1"`
			`VN="telnet"`
			`V1="permit"`
			or
			`UN="fred"`
			`VN="configure"`
			`V1="deny"`
			The first example permits the Telnet command to be authorized for users of Group 1. Any arguments can be supplied to the Telnet command as long as they are not matched against any defined via Action 176.
			The second example permits the **configure** command to be authorized for user fred, but only if the arguments supplied are permitted by the filter defined by a series of Action 176es.

175	REMOVE_IOS_ COMMAND	UN|GN, VN	Removes command authorization for the user or group:
			`GN="Group 1"`
			`VN="telnet"`
			or
			`UN="fred"`
			`VN="configure"`
			Users of Group 1 can no longer use the Cisco IOS **telnet** command.
			User fred can no longer use the **configure** command.

Downloaded from www.Manualslib.com manuals search engine

Table G-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description

176	ADD_IOS_ COMMAND_ ARG	UN|GN, VN, V1, V2	Specifies a set of command-line arguments that are either permitted or denied for the Cisco IOS command contained in VN. The command must have already been added via Action 174:
			`GN="Group 1"`
			`VN="telnet"`
			`V1="permit"`
			`V2="10.1.1.2"`
			or
			`UN="fred"`
			`VN="show"`
			`V1="deny"`
			`V2="run"`
			The first example will allow the **telnet** command with argument 10.1.1.2 to be used by any user in Group 1.
			The second example ensures that user fred cannot issue the Cisco IOS command **show run**.

177	REMOVE_IOS_ COMMAND_ ARG	UN|GN, VN, V2	Remove the permit or deny entry for the given Cisco IOS command argument:
			`GN="Group 1"`
			`VN="telnet"`
			`V2="10.1.1.1"`
			or
			`UN="fred"`
			`VN="show"`
			`V2="run"`

Downloaded from www.Manualslib.com manuals search engine

Table G-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description

178	SET_PERMIT_ DENY_ UNMATCHED_ IOS_ COMMANDS	UN|GN, V1	The default is that any Cisco IOS commands not defined via a combination of Actions 174 and 175 will be denied. This behavior can be changed so that issued Cisco IOS commands that do not match any command/command argument pairs are authorized:
			`GN="Group 1"`
			`V1="permit"`
			or
			`UN="fred"`
			`V1="deny"`
			The first example will permit any command not defined by Action 174.

179	REMOVE_ALL_ IOS_ COMMANDS	UN|GN	This action removes all Cisco IOS commands defined for a particular user or group.
210	RENAME_ GROUP	GN,V1	Renames an existing group to the name supplied in value 1.
211	RESET_GROUP	GN	Resets a group back to the factory default.
212	SET_VOIP	GN, V1	Enables or disables Voice over IP (VoIP) support for the group named, as follows: • GN = name of group • V1 = ENABLE or DISABLE

Action Codes for Modifying Network Configuration

Table G-6 on page G-28 lists the action codes for adding AAA clients, AAA servers, and network device groups, in addition to proxy table entries. Transactions using these codes affect the configuration displayed in the Network

Downloaded from www.Manualslib.com manuals search engine

Configuration section of the HTML interface. For more information about the Network Configuration section, see Chapter 4, "Setting Up and Managing Network Configuration."

Table G-6 Action Codes for Modifying Network Configuration

Action Code	Name	Required	Description

220	ADD_NAS	VN, V1, V2, V3	Add a new AAA client (named in VN) with an IP address (V1), shared secret key (V2), and vendor (V3). Valid vendors are as follows:
			• **VENDOR_ID_IETF_RADIUS**—For IETF RADIUS.
			• **VENDOR_ID_CISCO_RADIUS**—For Cisco IOS/PIX RADIUS.
			• **VENDOR_ID_CISCO_TACACS**—For Cisco TACACS+.
			• **VENDOR_ID_ASCEND_RADIUS**—For Ascend RADIUS.
			• **VENDOR_ID_ALTIGA_RADIUS**—For Cisco VPN 3000 RADIUS.
			• **VENDOR_ID_COMPATIBLE_RADIUS**—For Cisco VPN 5000 RADIUS.
			• **VENDOR_ID_AIRONET_RADIUS**—For Cisco Aironet RADIUS.
			• **VENDOR_ID_NORTEL_RADIUS**—For Nortel RADIUS.
			• **VENDOR_ID_JUNIPER_RADIUS**—For Juniper RADIUS.
			• **VENDOR_ID_CBBMS_RADIUS**—For Cisco BBMS RADIUS.
			For example:
			`VN = AS5200-11`
			`V1 = 192.168.1.11`
			`V2 = byZantine32`
			`V3 = VENDOR_ID_CISCO_RADIUS`

Downloaded from www.Manualslib.com manuals search engine

Table G-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
221	SET_NAS_ FLAG	VN, V1	For the named AAA client (VN) set one of the per-AAA client flags (V1). Use the action once for each flag required. Valid values for per-AAA client flags are as follows: • FLAG_SINGLE_CONNECT • FLAG_LOG_KEEP_ALIVE • FLAG_LOG_TUNNELS
222	DEL_HOST	VN	Delete the named AAA client (VN).
230	ADD_AAA_ SERVER	VN, V1, V2	Add a new AAA server named (VN) with IP address (V1), shared secret key (V2).
231	SET_AAA_ TYPE	VN, V1	Set the AAA server type for server (VN) to value in V1, which should be one of the following: • TYPE_ACS • TYPE_TACACS • TYPE_RADIUS The default is AAA_SERVER_TYPE_ACS
232	SET_AAA_ FLAG	VN, V1	For the named AAA server (VN) set one of the per-AAA client flags (V1): • FLAG_LOG_KEEP_ALIVE • FLAG_LOG_TUNNELS Use the action once for each flag required.
233	SET_AAA_ TRAFFIC_ TYPE	VN, V1	For the named AAA server (VN), set the appropriate traffic type (V1): • TRAFFIC_TYPE_INBOUND • TRAFFIC_TYPE_OUTBOUND • TRAFFIC_TYPE_BOTH The default is TRAFFIC_TYPE_BOTH.
234	DEL_AAA_ SERVER	VN	Delete the named AAA server (VN).

Downloaded from www.Manualslib.com manuals search engine

Table G-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
240	ADD_PROXY	VN, V1, V2, V3	Add a new proxy markup (VN) with markup type (V1) strip markup flag (V2) and accounting flag (V3). The markup type (V1) must be one of the following: • MARKUP_TYPE_PREFIX • MARKUP_TYPE_SUFFIX The markup strip flag should be TRUE if the markup is to be removed from the username before forwarding. The accounting flag (V3) should be one of the following: • ACCT_FLAG_LOCAL • ACCT_FLAG_REMOTE • ACCT_FLAG_BOTH
241	ADD_PROXY_ TARGET	VN, V1	Add to named proxy markup (VN) the host name (V1). The host should already be configured on the Cisco Secure ACS. The order in which proxy targets are added sets the proxy search order; the first target added is the first target proxied to, and so on. The order must be changed through the HTML interface.
242	DEL_PROXY	VN	Delete the named proxy markup (VN).
250	ADD_NDG	VN	Create a network device group (NDG) named (VN).
251	DEL_NDG	VN	Delete the named NDG.
252	ADD_HOST_TO _NDG	VN, V1	Add to the named AAA client/AAA server (VN) the NDG (V1).
300	RESTART_ PROTO_MODU LES	—	Restart the CSRadius and CSTacacs services to apply new settings.

Downloaded from www.Manualslib.com manuals search engine

Action Code for Deleting the CiscoSecure User Database

Table G-7 lists the action code for deleting all users and groups from the CiscoSecure user database.

Caution Using action code 200 irrevocably deletes all users and groups from the CiscoSecure user database. Before using this action code, we strongly recommend that you backup the CiscoSecure user database.

Table G-7 Action Code for Deleting the CiscoSecure User Database

Action Code	Name	Required	Description
200	DEL_CSDB	—	Delete all users and groups from the CiscoSecure user database. This code is particularly useful if you intend to rebuild the CiscoSecure user database using RDBMS synchronization.

Cisco Secure ACS Attributes and Action Codes

This section complements the previous section by providing an inverse reference; the following topics contain tables that list Cisco Secure ACS attributes, their data types and limits, and the action codes you can use to act upon the Cisco Secure ACS attributes:

- User-Specific Attributes, page G-31
- User-Defined Attributes, page G-34
- Group-Specific Attributes, page G-34

User-Specific Attributes

Table G-8 on page G-32 lists the attributes that define a Cisco Secure ACS user, including their data types, limits, and default values. It also provides the action code you can use in your accountActions table to affect each attribute. Although there are many actions available, adding a user requires only one transaction: ADD_USER. You can safely leave other user attributes at their default values. The

Downloaded from www.Manualslib.com manuals search engine

term NULL is not simply an empty string, but means not set; that is, the value will not be processed. Some features are processed only if they have a value assigned to them. For more information about action codes, see the "Action Codes" section on page G-5.

Table G-8 User-Specific Attributes

Attribute	Logical Type	Limits	Default	Actions
Username	String	1-64 characters	—	100, 101
ASCII/PAP Password	String	4-32 characters	Random string	100, 102
CHAP Password	String	4-32 characters	Random string	103
Outbound CHAP Password	String	4-32 characters	NULL	104
TACACS+ Enable Password	String Password	4-32 characters	NULL	105
Integer privilege level	0-15 characters	NULL		
Group	String	0-100 characters	"Default Group"	106
Password Supplier	Enum	See Table G-3 on page G-7.	LIBRARY_ CSDB	107
Password Type	Enum	See Table G-3 on page G-7.	PASS_TYPE _CSDB (password is cleartext PAP)	108
Password Expiry Status	Bitwise Enum	See Table G-3 on page G-7.	PASS_ STATUS_ NEVER (never expires)	109, 110
Expiry Data	Short wrong max/current	0-32,767	—	112, 113
Expiry date	—	—		

Downloaded from www.Manualslib.com manuals search engine

Table G-8 User-Specific Attributes (continued)

Attribute	Logical Type	Limits	Default	Actions
Max Sessions	Unsigned short	0-65535	MAX_SESSIONS_AS_GROUP	114
TODDOW Restrictions	String	168 characters	111111111111	140
NAS Access Control	Bool enabled	T/F	NULL	120, 122
Bool permit/deny	T/F			
ACL String (See Table G-4 on page G-16.)	0-31 KB			
Dial-Up Access Control	Bool enabled	T/F	NULL	121, 123
Bool permit/deny	T/F	NULL		
ACL String (See Table G-4 on page G-16.)	0-31 KB	NULL		
Static IP Address	Enum scheme	(See Table G-4 on page G-16.)	Client	150
String IP/Pool name	0-31 KB	NULL		
Callback Number	String	0-31 KB	NULL	151
TACACS Attributes	Formatted String	0-31 KB	NULL	160, 162
RADIUS Attributes	Formatted String	0-31 KB	NULL	170, 173
UDF 1	String Real Name	0-31 KB	NULL	1, 2
UDF 2	String Description	0-31 KB	NULL	1, 2
UDF 3	String	0-31 KB	NULL	1, 2
UDF 4	String	0-31 KB	NULL	1, 2
UDF 5	String	0-31 KB	NULL	1, 2

Downloaded from www.Manualslib.com manuals search engine

User-Defined Attributes

User-defined attributes (UDAs) are string values that can contain any data, such as social security number, department name, telephone number, and so on. You can configure Cisco Secure ACS to include UDAs on accounting logs about user activity. For more information about configuring UDAs, see "User Data Configuration Options" section on page 3-3.

RDBMS Synchronization can set UDAs by using the SET_VALUE action (code 1) to create a value called "USER_DEFINED_FIELD_0" or "USER_DEFINED_FIELD_1". For accountActions rows defining a UDA value, the AppId (AI) field must contain "APP_ CSAUTH" and the Value2(V2) field must contain "TYPE_STRING".

Table G-9 lists the data fields that define UDAs. For more information about action codes, see the "Action Codes" section on page G-5.

Table G-9 User-Defined Attributes

Action	Username (UN)	ValueName (VN)	Value1 (V1)	Value2 (V2)	AppId (AI)
1	fred	USER_DEFINED_FIELD_0	SS123456789	TYPE_STRING	APP_CSAUTH
1	fred	USER_DEFINED_FIELD_1	Engineering	TYPE_STRING	APP_CSAUTH
1	fred	USER_DEFINED_FIELD_2	949-555-1111	TYPE_STRING	APP_CSAUTH

Note If more than two UDAs are created, only the first two are passed to accounting logs.

Group-Specific Attributes

Table G-10 on page G-35 lists the attributes that define a Cisco Secure ACS group, including their data types, limits, and default values. It also provides the action code you can use in your accountActions table to affect each field. For more information about action codes, see the "Action Codes" section on page G-5.

Downloaded from www.Manualslib.com manuals search engine

Table G-10 Group-Specific Attributes

Attribute	Logical Type	Limits	Default	Actions
Max Sessions	Unsigned short	0-65534	MAX_SESSIONS_UNLIMITED	114
Max Sessions for user of group	Unsigned short	0-65534	MAX_SESSIONS_UNLIMITED	115
Token caching for session	Bool	T/F	NULL	130
Token caching for duration	Integer time in seconds	0-65535	NULL	131
TODDOW Restrictions	String	168 characters	111111111111	140
NAS Access Control	Bool enabled	T/F	NULL	120, 122
Bool permit/deny	T/F			
ACL String (See Table G-4 on page G-16.)	0-31 KB			
Dial-Up Access Control	Bool enabled	T/F	NULL	121, 123
Bool permit/deny	T/F	NULL		
ACL String (See Table G-4 on page G-16.)	0-31 KB	NULL		
Static IP Address	Enum scheme	(See Table G-4 on page G-16.)	Client	150
String IP/Pool name	0-31 KB	NULL		
TACACS Attributes	Formatted String	0-31 KB	NULL	160, 162
RADIUS Attributes	Formatted String	0-31 KB	NULL	170, 173
VoIP Support	Bool disabled	T/F	NULL	212

Downloaded from www.Manualslib.com manuals search engine

An Example accountActions Table

Table G-11 presents an example of an accountActions table that contains some of the action codes described in Action Codes, page G-5. First user "fred" is created, along with his passwords, including a TACACS_ Enable password with privilege level 10. Fred is assigned to "Group 2." His account expires after December 31, 1999, or after 10 incorrect authentication attempts. Attributes for Group 2 include Time-of-Day/Day-of-Week restrictions, token caching, and some RADIUS attributes.

Note This example omits several columns that should appear in any accountActions table. The omitted columns are Sequence ID (SI), Priority (P), DateTime (DT), and MessageNo (MN).

Table G-11 Example accountActions Table

Action	User name (UN)	Group Name (GN)	Value Name (VN)	Value1 (V1)	Value2 (V2)	Value3 (V3)	AppId (AI)
100	fred	—	—	fred	—	—	—
102	fred	—	—	freds_password	—	—	—
103	fred	—	—	freds_chap_ password	—	—	—
104	fred	—	—	freds_outbound_ password	—	—	—
105	fred	—	—	freds_enable_ password	10	—	—
106	fred	Group 2	—	—	—	—	—
150	fred	—	—	123.123.123.123	—	—	—
151	fred	—	—	01832-123900	—	—	—
109	fred	—	—	PASS_STATUS_ NEVER	—	—	—
110	fred	—	—	PASS_STATUS_ WRONG	—	—	—

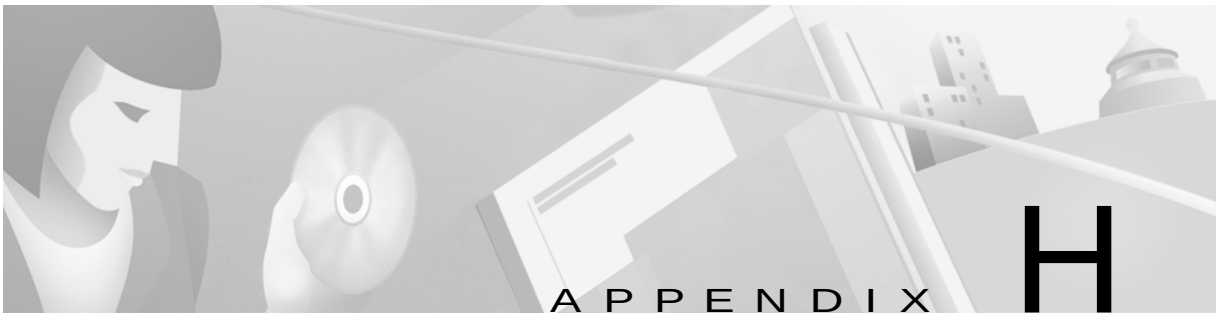
Downloaded from www.Manualslib.com manuals search engine

Table G-11 Example accountActions Table (continued)

Action	User name (UN)	Group Name (GN)	Value Name (VN)	Value1 (V1)	Value2 (V2)	Value3 (V3)	AppId (AI)
110	fred	—	—	PASS_STATUS_ EXPIRES	—	—	—
112	fred	—	—	10	—	—	—
113	fred	—	—	19991231	—	—	—
114	fred	—	—	50	—	—	—
115	fred	—	—	50	—	—	—
120	fred	—	—	ACCESS_PERMIT	—	—	—
121	fred	—	—	ACCESS_DENY	—	—	—
122	fred	—	—	NAS01,tty0, 01732-975374	—	—	—
123	fred	—	—	01732-975374, 01622-123123	CLID/ DNIS	—	—
1	fred	—	USER_ DEFINED_ FIELD_0	Fred Jones	TYPE_ STRING	—	APP_CSAUTH
140	—	Group 2	—	[a string of 168 ones (1)]	—	—	—
130	—	Group 2	—	DISABLE	—	—	—
131	—	Group 2	—	61	—	—	—
163	—	Group 2	Reply-Message	Welcome to Your Internet Service	—	—	—
163	—	Group 2	Vendor-Specific	addr-pool=pool2	9	1	—

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine



Cisco Secure ACS Internal Architecture

Cisco Secure Access Control Server for Windows NT/2000 Servers Version 3.0 (Cisco Secure ACS) is designed to be modular and flexible to fit the needs of both simple and large networks. This chapter describes the Cisco Secure ACS architectural components. Cisco Secure ACS includes the following service modules:

- CSAdmin
- CSAuth
- CSDBSync
- CSLog
- CSMon
- CSTacacs
- CSRadius

Each module can be started and stopped individually from within the Microsoft Service Control Panel or as a group from within the Cisco Secure ACS HTML interface. Each module can operate independently, but this limits functionality.

Downloaded from www.Manualslib.com manuals search engine

Windows NT/2000 Environment Overview

This section gives a brief overview of essential Windows NT/2000 concepts that relate to Cisco Secure ACS as a service of Windows NT/2000.

Windows NT/2000 Services

All Cisco Secure ACS services can be started, stopped, and restarted from the Windows NT/2000 Services window. The Cisco Secure ACS services are preceded by the letters CS. The sorting mechanism within Windows NT/2000 Services lists services alphabetically. All Cisco Secure ACS services should be displayed in one area of the list.

Windows NT/2000 Registry

The Windows NT/2000 Registry is a tree-like storage area for all application information.

Note We recommend that you do not modify this file unless you have enough knowledge and experience to edit the file without destroying any existing data in the file. Always back up the Windows Registry before editing.

The Cisco Secure ACS information is located in the following Windows Registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\CISCO
```

Cisco Secure ACS Web Server

Cisco Secure ACS has a built-in web server for support using a hypertext markup language (HTML) interface. This eliminates the necessity of installing another web server on the Windows NT/2000 server running Cisco Secure ACS. Because the Cisco Secure ACS web server uses port 2002, you can use another web server on the same machine to provide other web services.

Downloaded from www.Manualslib.com manuals search engine

CSAdmin

CSAdmin is the service for the internal web server. Cisco Secure ACS does not require the presence of a third-party web server; it is equipped with its own internal server. After Cisco Secure ACS is installed, you must configure it from its HTML interface. This means that CSAdmin must be running when you configure Cisco Secure ACS.

Although you can start and stop services from within the Cisco Secure ACS HTML interface, this does not include starting or stopping CSAdmin. If CSAdmin stops abnormally because of an external action, you cannot access Cisco Secure ACS from any machine other than the Windows NT/2000 server on which it is running. You can start or stop CSAdmin from the Windows NT/2000 Service menu.

CSAdmin is a multithreaded application that enables several administrators to access it at the same time. Therefore, CSAdmin is best for distributed, multiprocessor, and clustered environments.

Note When you access CSAdmin from a browser, a new port is assigned for that session of the browser. This increases security and helps with session management. Therefore, when a firewall is used with authentication forwarding, you must exclude the *server IP address*:2002 port.

CSAuth

CSAuth is the authentication and authorization service. Its primary purpose is the authentication and authorization of requests to permit or deny access to users. CSAuth determines if access should be granted and defines the privileges for a particular user. CSAuth is the database manager.

Cisco Secure ACS can access several different databases for authentication. When a request for authentication arrives, Cisco Secure ACS checks the database that is configured for that user. If the user is unknown, Cisco Secure ACS checks the database(s) configured for unknown users.

Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS can check the user database to authenticate first-time logins. If the username is not in the CiscoSecure user database, Cisco Secure ACS does not deny authentication yet; it forwards the request to the configured unknown user database to see if it can authenticate the user. If it can, authentication is granted.

Note With unknown user databases such as Windows NT/2000 and Novell NDS, only PAP passwords are supported.

There are several user database options:

- **CiscoSecure user database—**The first database option provides the fastest response time for authentication. Locating the username and checking the password against the local CiscoSecure user database is a single step. Because this occurs internally to Cisco Secure ACS, there is no delay while Cisco Secure ACS waits for a response from an external user database.
- **Windows NT/2000 user database—**This option makes use of the work invested in the Windows NT/2000 user database. CSAuth passes the username and password to Windows NT/2000 for authentication. Windows NT/2000 then provides a response approving or denying validation. If the response is approval, CSAuth knows that the user should be allowed to authenticate.

  If the response is denial and the username was submitted to Cisco Secure ACS in an unqualified format (that is, without a domain name preceding the username), CSAuth tries each Windows NT domain in the order they are configured in the Domain List list box in External User Databases: Windows NT/2000: Configure.
- **Novell NDS option—**This option allows Cisco Secure ACS to use the Novell NDS service to authenticate users. Cisco Secure ACS supports one Tree, but the Tree can have multiple Containers and Contexts. To support this compatibility, the Novell requester must be installed on the same Windows NT/2000 server as Cisco Secure ACS.
- **Third-party token servers—**Cisco Secure ACS supports several third-party token servers, such as RSA SecurID, SafeWord AXENT, and any hexadecimal X.909 token card such as CRYPTOCard. For some token servers, Cisco Secure ACS acts as a client to the token server. For others, it uses the token server's RADIUS interface for authentication requests. As with the Windows NT/2000 database, after the username is located in the CiscoSecure user database, CSAuth can check the selected token server to

Downloaded from www.Manualslib.com manuals search engine

verify the username and token-card password. The token server then provides a response approving or denying validation. If the response is approval, CSAuth knows that authentication should be granted for the user.

- **Generic LDAP—**Cisco Secure ACS supports authentication of users against records kept in a directory server through the Lightweight Directory Access Protocol (LDAP). Cisco Secure ACS interacts with the most popular directory servers, including Novell and Netscape. Both PAP and CHAP passwords can be used when authenticating against the LDAP database. Cisco Secure ACS logs these transactions and displays their results in the Reports & Activity section of the Cisco Secure ACS HTML interface.
- **ODBC—**Cisco Secure ACS supports authentication via an Open Database Connectivity (ODBC)-compliant SQL database. ODBC is a standardized API that was first developed by Microsoft and is now used by most major database vendors. ODBC follows the specifications of the SQL Access Group. The benefit of ODBC in a web-based environment is easy access to data storage programs such as Microsoft Access and SQL Server.
- **UNIX passwords—**Cisco Secure ACS includes a password import utility you can use to import passwords from a UNIX database. From the Cisco Secure ACS directory, type the following command:

  `CSUtil.exe -i filename`

  where *filename* is the name of a text file that contains the following line for each user:

  `ADD:username:UNIX:DES-encrypted password`

  For example:

  `ADD:roger:UNIX:kk/amz1NUJrlM`

For more information on CSUtil.exe, see Appendix E, “Cisco Secure ACS Command-Line Database Utility.”

When a user has authenticated using one of the described methods, Cisco Secure ACS obtains a set of authorizations from the user profile and the group to which the user is assigned. This information is stored with the username in the CiscoSecure user database. Some of the authorizations included are the services to which the user is entitled, such as IP over PPP, IP pools from which to draw an IP address, access lists, and password aging information. The authorizations, with the approval of authentication, are then passed to the CSTacacs or CSRadius modules to be forwarded to the requesting device.

Downloaded from www.Manualslib.com manuals search engine

CSDBSync

CSDBSync is the service used to synchronize the Cisco Secure ACS database with third-party RDBMS systems and is an alternative to using the ODBC dynamic link library (DLL). Starting with Version 2.4, CSDBSync synchronizes AAA client, AAA server, network device groups (NDGs) and Proxy Table information. For information on relational database management system (RDBMS) synchronization, see the "RDBMS Synchronization" section on page 8-24.

CSLog

CSLog is the service used to capture and place logging information. CSLog gathers data from the TACACS+ or RADIUS packet and CSAuth, and then manipulates the data to be placed into the comma-separated value (CSV) files. By default, the CSV files are created daily at midnight, but beginning with Version 2.3, the CSV files can be created daily, weekly, monthly, or by file size. The CSV files can be imported into spreadsheets that support this format.

CSV files are stored in the default subdirectory `\Program Files\Cisco Secure ACS v`*`x.x`*`\`Logs\. There are 10 subdirectories that contain CSV files:

- **AdminAudit—**Contains the log files of administrator activity
- **Backup and Restore—**Contains the log files of ACS system backup and restore activity
- **DBReplicate—**Contains the log files of database replication activity
- **DbSync—**Contains the log files of RDBMS synchronization activity
- **Failed Attempts—**Contains the log files of failed authentication attempts information
- **RADIUS Accounting—**Contains the log files of successful authentication and authorization activity for RADIUS users
- **Service Monitoring—**Contains the log files of service activities
- **TACACS+ Accounting—**Contains the log files of successful authentication and authorization activity for TACACS+ users

Downloaded from www.Manualslib.com manuals search engine

- **TACACS+ Administration—**Contains the log files of TACACS+ administration events
- **VoIP Accounting—**Contains the log files of successful authentication and authorization activity for Voice over IP (VoIP) users

CSMon

CSMon is a service provided as a part of Cisco Secure ACS that facilitates minimum down time in a remote access network environment. CSMon performs four basic activities:

- **Monitoring—**Monitors the overall status of Cisco Secure ACS and the system on which it is running
- **Recording—**Records and reports all exceptions to a special log file
- **Notification—**Alerts the administrator to potential problems and real events regarding Cisco Secure ACS and records all such problems
- **Response—**Attempts to automatically and intelligently fix detected problems

CSMon works for both TACACS+ and RADIUS and automatically detects which protocols are in use.

Note CSMon is not intended as a replacement for system, network, or application management applications but is provided as an application-specific utility that can be used with other, more generic system management tools.

Monitoring

CSMon actively monitors three basic sets of system parameters:

- Generic host system state—Windows NT/2000 itself provides several built-in utilities, such as the Event Log and Performance Monitor, to monitor overall system health, and there are several commercial applications available. CSMon monitors a small number of additional key system thresholds:
- Available space on the system hard disk (the drive with the Windows NT/2000 directory).

Downloaded from www.Manualslib.com manuals search engine

- Available space on Cisco Secure ACS installation drive
- Processor utilization
- Physical memory utilization

  All events related to generic host system state are categorized as "warning events".

- Application-specific performance—
  - Application viability—CSMon periodically performs a test login using a special built-in test account (the default period is one minute). Problems with this authentication can be used to determine if the ACS service has been compromised.
  - Application performance thresholds—CSMon monitors and records the latency of each test authentication request (the time it takes to receive a positive response). Each time this is performed, CSMon updates a variable containing the average response time value. Additionally, it records whether retries were necessary to achieve a successful response. By tracking the average time for each test authentication, CSMon can build up a “picture” of expected response time on the system in question. CSMon can therefore detect whether excess re-tries are required for each authentication or if response times for a single authentication exceed a percentage threshold over the average.
- System resource consumption by Cisco Secure ACS—CSMon periodically monitors and records the usage by Cisco Secure ACS of a small set of key system resources and compares it against predetermined thresholds for indications of atypical behavior. The parameters monitored include the following:
- Handle counts
- Memory utilization
- Processor utilization
- Thread used
- Failed log-on attempts

CSMon cooperates with CSAuth to keep a track of user accounts being disabled by exceeding their failed attempts count maximum. This feature is more oriented to security and user support than system viability. If configured, it provides

Downloaded from www.Manualslib.com manuals search engine

immediate warning of "brute force" attacks by alerting the administrator to a large number of accounts becoming disabled. In addition, it facilitates a support help desk to anticipate problems with individual users gaining access.

Recording

CSMon records all exception events in logs that you can use to diagnose problems. CSMon puts the logs in two places, sends notification(s), and responds:

- CSMon Log—Like the other Cisco Secure ACS components, CSMon maintains a CSV log of its own for diagnostic and error logging. Because this logging consumes relatively small amounts of resources, CSMon logging cannot be disabled.
- Windows NT/2000 Event Log—In addition to the native CiscoSecure service logging, CSMon logs all messages to the Windows NT/2000 Event Log. Logging to the Windows NT/2000 Event Log is enabled by default but can be disabled.
- Notification—CSMon can be configured to notify system administrators in the following cases:
- Exception events (including the current state of Cisco Secure ACS)
- Response
- Outcome of the response (including the current state of Cisco Secure ACS)

  The default notification method is simple mail-transfer protocol (SMTP) e-mail, but you can create scripts to enable other methods.
- Response—CSMon detects exception events that affect the integrity of the service. Monitored events are listed above. These events are application-specific and hard-coded into Cisco Secure ACS. There are two types of responses:
  - Warning events—Service is maintained but some monitored threshold is breached
  - Failure events—One or more Cisco Secure ACS components stop providing service

Downloaded from www.Manualslib.com manuals search engine

CSMon responds to the event by logging the event, sending notifications (if configured) and, if the event is a failure, taking action. There are two types of actions:

– Predefined actions—These actions are hard-coded into the program and are always carried out when a triggering event is detected. Because these actions are hard-coded, they are integral to the application and do not need to be configured. These actions include running the CSSupport utility, which captures most of the parameters dealing with the state of the system at the time of the event.

  If the event is a warning event, it is logged and the administrator is notified. No further action is taken. CSMon also attempts to fix the cause of the failure after a sequence of re-tries and individual service restarts.

– User Definable Actions—If the predefined actions built into CSMon do not fix the problem, CSMon can execute an external program or script. A number of sample scripts are provided to perform such functions as application restart, or you can create your own.

Sample Scripts

The following scripts are provided with CSMon:

- **RESTART_ALL_SERVICES.BAT—**Restarts all Cisco Secure ACS services
- **RESTART_PROTOCOL_MODULES.BAT—**Restarts just the protocol modules (CSTacacs+ and CSRadius)
- **REBOOT.BAT—**Reboots the Cisco Secure ACS system

Configuration

You can configure the following items through CSAdmin:

- **Test login frequency—**Defines the frequency with which CSMon attempts to perform its built-in test authentication. The default period is every 60 seconds. You can disable test authentications or set the frequency higher; however, the overhead generated by this feature is small and there is no real benefit from setting it higher.

Downloaded from www.Manualslib.com manuals search engine

- **Script to execute in the event of a failure event—**These scripts are normally standard Windows NT/2000 .BAT batch command files, but you can use any executable in the `Program Files\CiscoSecure ACS v2.6\CSMon\Scripts` directory.
- **Windows NT/2000 Event Log enable/disable—**By default, CSMon logs events to the Windows NT/2000 Event Log, but you can disable this function. CSV logging cannot be disabled.
- **Simple mail-transfer protocol (SMTP) server and administrator e-mail account details—**To enable Cisco Secure ACS to send e-mail notification of error conditions, you must fill in these fields. You can enter any valid e-mail account (joe@company.com). The server details can be either a qualified host name or a valid IP address. CSMon does not verify delivery of notification e-mails, so make sure the information in these fields is correct. To disable notification, clear the check box.

CSTacacs and CSRadius

The CSTacacs and CSRadius services communicate between the CSAuth module and the access device that is requesting authentication and authorization services. For CSTacacs and CSRadius to work properly, the system must meet the following conditions:

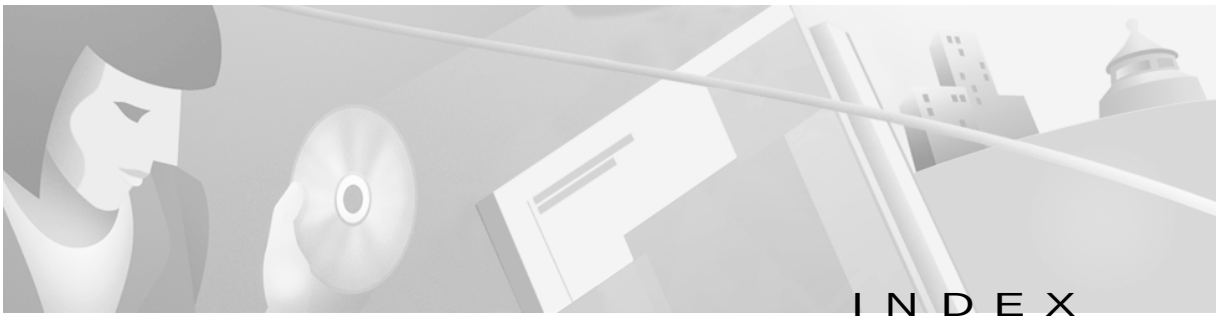
- CSTacacs and CSRadius services must be configured from CSAdmin.
- CSTacacs and CSRadius services must communicate with access devices such as access servers, routers, switches, and firewalls.
- The identical shared secret (key) must be configured both in Cisco Secure ACS and on the access device.
- The access device IP address must be specified in Cisco Secure ACS.
- The type of security protocol being used must be specified in Cisco Secure ACS.

CSTacacs is used to communicate with TACACS+ devices and CSRadius to communicate with RADIUS devices. Both services can run at the same time. When only one security protocol is used, only the applicable service needs to be running; however, the other service will not interfere with normal operation and

Downloaded from www.Manualslib.com manuals search engine

does not need to be disabled. See Appendix C, "TACACS+ Attribute-Value Pairs" for more information on TACACS+ AV pairs, or Appendix D, "RADIUS Attributes" for more information on RADIUS+ AV pairs.

Downloaded from www.Manualslib.com manuals search engine



INDEX

A

AAA
- definition 1-1
- pools
  - IP addresses assigned from 7-12

AAA clients
- adding and configuring 4-9
- definition 1-5
- deleting 4-14
- editing 4-12
- interaction with AAA servers 1-5
- IP Pools 7-12
- supported Cisco AAA clients 1-2
- timeout 12-7
- timeout values 12-6

AAA Clients table 4-1

AAA servers
- adding 4-16
- configuring 4-16
- deleting 4-20
- editing 4-18
- enabling in interface (table) 3-5
- in distributed systems 4-3
- master 8-7
- overview 4-15
- primary 8-7
- replicating 8-7
- secondary 8-7
- troubleshooting A-1

access devices 1-5

accessing Cisco Secure ACS
- how to 1-26
- URL 1-24

access policies
- in Administration Control 10-10

account disablement
- Account Disabled check box 7-6
- setting options for 7-21

accounting
- overview 1-17

accounts
- disabling manually 7-53

ACLs
- See downloadable PIX ACLs

ACS Backup and Restore log
- CSV file directory 9-15
- overview 9-15
- viewing 9-20

Downloaded from www.Manualslib.com manuals search engine

ACS backups
See backups
ACS service management
event logging
configuring 8-51
overview 8-48
system monitoring
configuring 8-50
custom actions 8-50
ACS Service Monitoring log
CSV file directory 9-35
overview 9-18
viewing 9-20
ACS system restore
See restore
action codes
in accountActions table G-5
ActivCard user databases
configuring 11-50
group mappings 12-10
RADIUS-based group specification 12-21
Administration Audit log
configuring 9-17
CSV file directory 9-17
overview 9-17
viewing 9-20
Administration Control
audit policy setup 10-16
session policies 10-13
administrative access policies 2-14
administrators
adding 10-6
deleting 10-9
editing 10-7
troubleshooting A-2
age-by-date rules
in Group Setup 6-23
ARAP
compatible databases 1-9
in User Setup 7-6
protocol supported 1-10
ASCII/PAP
compatible databases 1-9
protocol supported 1-10
attributes
enabling in interface 3-2
group-specific (table) G-34
per-group 3-2
per-user 3-2
user-defined
logging 9-2
user-specific (table) G-34
attribute-value pairs
See AV pairs
audit policies
overview 10-16
authentication
configuration 8-73

Downloaded from www.Manualslib.com manuals search engine

overview 1-7
authorization
overview 1-15
AV pairs
RADIUS
Ascend D-21
Cisco IOS D-3
IETF D-12
IETF accounting D-16
IETF vendor-proprietary D-10
overview D-1
See also RADIUS VSAs
TACACS+
accounting C-4
general C-1
AXENT user databases
configuring external databases 11-55
group mappings 12-10

B

Backup and Restore log directory
See ACS Backup and Restore log
backups
components backed up 8-41
directory management 8-41
filenames 8-45
locations 8-41
overview 8-40
reports 8-42
scheduled vs. manual 8-40
scheduling 8-43
vs. replication 8-11
with CSUtil.exe E-5
browsers
troubleshooting A-3

C

cached users 12-2
caching
password configuration 1-12
callback options
in Group Setup 6-6
in User Setup 7-10
certificate setup in ACS 8-61
certificate trust list 8-70
certification
adding new CAs 8-72
authority 8-70
automatic enrollment 8-68
backups 8-41
generating requests for 8-64
manual enrollment 8-66
models 8-71
replacement 8-69
update 8-69

Downloaded from www.Manualslib.com manuals search engine

CHAP
compatible databases 1-9
in User Setup 7-6
protocol supported 1-10
CHAP/MS-CHAP/ARAP
in User Setup 7-6
Cisco.com
accessing xxxiv
overview xxxiii
Cisco IOS
RADIUS
AV pairs D-2
group attributes 6-36
user attributes 7-38
TACACS+
AV pairs C-1
troubleshooting A-4
CiscoSecure authentication agent 1-14, 6-20
CiscoSecure database replication
See replication
CiscoSecure user database
option in CSAuth H-4
overview 11-2
See also databases
command authorization sets
adding 5-15
configuring 5-12, 5-14
deleting 5-17
editing 5-17
overview 5-13
PIX command authorization sets 5-13
command-line database utility
See CSUtil.exe
CRYPTOCard user databases
configuring 11-50
group mappings 12-10
RADIUS-based group specification 12-21
CSAdmin H-3
CSAuth H-3
CSDBSync 8-25, H-6
CSLog H-6
CSMon
configuration H-10
functions H-7
log H-9
overview H-7
predefined actions H-10
sample scripts H-10
See also ACS service management
CSNTacctInfo 11-37, 11-39
CSNTAuthUserPap 11-35
CSNTerrorString 11-37, 11-39
CSNTExtractUserClearTextPw 11-36
CSNTgroup 11-37, 11-39
CSNTpassword 11-37, 11-39
CSNTresult 11-37, 11-39
CSNTusername 11-37, 11-38
CSRadius H-11

Downloaded from www.Manualslib.com manuals search engine

CSTacacs H-11
CSUtil.exe
  decoding error numbers with E-25
  import text files
    example E-22
  overview E-1
CSV log files
  downloading 9-21
custom attributes
  in user-level TACACS+ settings 7-24

D

database group mappings
  configuring
    for token servers 12-12
    for Windows NT/2000 domains 12-17
    no access groups 12-15
    order 12-20
  deleting
    group set mappings 12-18
    Windows NT/2000 domain configurations 12-19
  in external user databases 12-10
  overview 12-10
Database Replication log
  CSV file directory 9-16
  overview 9-16
  viewing 9-20
databases
  CiscoSecure user database 11-2
  deleting 11-58
  deployment considerations 2-17
  dump files E-9
  group mappings
    See database group mappings
  performance 12-6
  replication
    See replication
  search order 12-8
  search process 12-7, 12-8
  selecting user databases 11-1
  synchronization
    See RDBMS synchronization
  token cards
    See token servers
  troubleshooting A-5, A-15
  types
    See ActivCard user databases
    See AXENT user databases
    See CRYPTOCard user databases
    See generic LDAP user databases
    See LEAP proxy RADIUS user databases
    See Novell NDS user databases
    See ODBC features
    See RADIUS user databases
    See RSA user databases
    See SafeWord user databases

Downloaded from www.Manualslib.com manuals search engine

unknown users 12-1
user
See CiscoSecure user database
Windows NT user database
See Windows NT/2000 operating systems
data source name
for RDMBS synchronization 8-34
data source names
using with ODBC databases 11-30, 11-42
date format control
in System Configuration 8-3
DbSync log directory 9-16
debug logs
detail levels 9-35
frequency 9-35
troubleshooting A-11
default group
in Group Setup 6-2
default time-of-day/day-of-week specification
enabling in interface 3-4
default time-of-day access settings
in Group Setup 6-5
deleting logged-in users 9-12
deployment
overview 2-1
sequence 2-18
device groups
See network device groups
DHCP
with IP pools 8-53
dial-in
troubleshooting A-6
dial-up networking clients 11-9
digital certificates
See certification
Disabled Accounts report
overview 9-14
viewing 9-14
distributed systems
AAA servers in 4-3
overview 4-2
settings
configuring 4-25
default entry 4-3
enabling in interface 3-5
distribution table
See Proxy Distribution Table
documentation
conventions xxx
objectives xxvii
obtaining xxxii
organization xxviii, xxix
domain lists
configuring 11-13
inadvertent user lockouts 11-11
overview 11-11

Downloaded from www.Manualslib.com manuals search engine

downloadable PIX ACLs
adding 5-3
assigning to groups 6-27
assigning to users 7-22
configuring 5-3
deleting 5-5
enabling in interface
group-level 3-5
user-level 3-4
overview 5-2
draft-ietf-radius-tunnel-auth 1-6
dump files
databases
creating with CSUtil.exe E-9
exception events H-9
monitoring system health H-7
event logging
configuring 8-51
exception events H-9
exports
with CSUtil.exe E-2
external token servers
See token servers
external user databases
configuring 11-4
search order 12-8
See also databases
supported 1-8

E

EAP-TLS
authentication configuration 8-73
compatible databases 1-9
enable control
in TACACS+ interface configuration 7-32
enable password
in User Setup 7-34
error messages B-1
error numbers
decoding with CSUtil.exe E-25
Event log
disable H-11

F

Failed Attempts log
configuring
CSV 9-22
ODBC 9-27
CSV file directory 9-9
enabling
CSV 9-19
ODBC 9-27
viewing 9-20
failed log-on attempts H-8
failure events H-9
fallback on failed connection 4-2

Downloaded from www.Manualslib.com manuals search engine

finding users 7-52
firewalls
  administering AAA servers through 1-19
  troubleshooting A-16

G

gateways F-3
generic LDAP user databases
  authentication 11-14
  configuring 11-19
  directed authentications 11-17
  mappings
    database group to a AAA group 12-13
  organizational units and groups 11-17
  supported databases H-5
  supported protocols 1-10
grant dial-in permission to user 11-8, 11-13
greeting after login 6-23
group-level
  enabling in interface
    downloadable PIX ACLs 3-5
    network access restrictions 3-5
    network access restriction sets 3-5
    password aging 3-5
group-level network access restrictions
  See network access restrictions
groups
  assigning users to 7-9
  configuring RADIUS settings for
    See RADIUS
  Default Group 6-2
  enabling VoIP support for 6-4
  listing all users in 6-48
  mapping order 12-20
  mappings 12-10, 12-13
  multiple mappings 12-13
  no access groups
    for group set mappings 12-14
  overriding settings 3-2
  relationship to users 3-2
  renaming 6-49
  resetting usage quota counters for 6-49
  See also network device groups
  settings for
    callback options 6-6
    configuration-specific 6-15
    configuring common 6-3
    IP address assignment method 6-26
    max sessions 6-11
    network access restrictions 6-7
    password aging rules 6-20
    shell command authorization sets 6-30
    TACACS+ 6-28
    time-of-day access 6-5
    token cards 6-17
    usage quotas 6-13
  setting up and managing 6-1

Downloaded from www.Manualslib.com manuals search engine

sort order within group mappings 12-13
specification by ODBC authentication 11-37, 11-39
TACACS+ settings in 6-2

H

handle counts H-8
hard disk space H-7
hardware requirements 2-2
Help 1-23
host system state H-7
HTML interface
overview 1-21
See also Interface Configuration
web server H-2
HTTP port allocation
configuring 10-12
overview 1-19

I

importing passwords H-5
imports
with CSUtil.exe E-13
inbound authentication 1-12
inbound passwords
configuration 1-12
installation
related documentation xxxi
system requirements 2-2
troubleshooting A-13
Interface Configuration
advanced options 3-4
configuring 3-1
customized user data fields 3-3
security protocol options 3-9
IP addresses
in User Setup 7-11
requirement for CSTacacs and CSRadius H-11
setting assignment method for user groups 6-26
IP pools
DHCP 8-53
enabling in interface 3-5
overlapping 8-53, 8-55
See also IP pools address recovery
See also IP pools server
user IP addresses 7-12
IP pools address recovery
configuring 8-59
in System Configuration 8-59
IP pools server
adding IP pools 8-55
overview 8-52

Downloaded from www.Manualslib.com manuals search engine

L

LAN manager 1-11
LEAP proxy RADIUS user databases
  configuring external databases 11-45
  group mappings 12-10
  RADIUS-based group specification 12-21
list all users
  in Group Setup 6-48
  in User Setup 7-51
Logged-In Users report
  deleting logged-in users 9-12
  overview 9-11
  viewing 9-11
logging
  configuring 9-23
  CSV files 9-1
  debug logs
    detail levels 9-35
    frequency 9-35
  domain names 9-2
  external user databases 9-2
  ODBC logs
    enabling in interface 3-6
    overview 9-1
  remote logging
    configuring 9-32
    enabling in interface 3-5
    logging hosts 9-30
    overview 9-30
  See also logs
  See also reports
  service logs
    configuring 9-35
  services
    list of logs generated 9-34
  system logs 9-15
  troubleshooting A-14
  user-defined attributes 9-2
  watchdog packets 9-3
login frequency
  internal testing H-10
logins
  greeting upon 6-23
logs
  See ACS Backup and Restore log
  See ACS Service Monitoring log
  See Administration Audit log
  See Database Replication log
  See Failed Attempts log
  See logging
  See Passed Authentications log
  See RADIUS Accounting log
  See RDBMS Synchronization log
  See reports
  See TACACS+ Accounting log
  See TACACS+ Administration log
  See VoIP Accounting log

Downloaded from www.Manualslib.com manuals search engine

M

mappings
database groups to AAA groups 12-13
database to AAA groups 12-10
master AAA servers 8-7
max sessions
enabling in interface 3-5
in Group Setup 6-11
in User Setup 7-17
overview 1-16
troubleshooting A-13
memory utilization H-8
Microsoft Access H-5
Microsoft SQL Server H-5
monitoring
configuring 8-50
CSMon H-7
overview 8-49
MS-CHAP
compatible databases 1-9
configuring 8-73
overview 1-11
protocol supported 1-10
multiple group mappings 12-13

N

NAR
See network access restrictions
NAS
See AAA clients
NDG
See network device groups
NDS
See Novell NDS user databases
network access filters
See network access restrictions
network access quotas
overview 1-16
network access restrictions
adding 5-8
configuring 5-7
deleting 5-12
editing 5-4, 5-10
enabling in interface
group-level 3-5
user-level 3-4
in Group Setup 6-7
interface configuration 3-5
in User Setup 6-7, 7-12
overview 5-6
network access restriction sets
enabling in interface
group-level 3-5

Downloaded from www.Manualslib.com manuals search engine

network access servers
See AAA clients
Network Configuration 4-1
network device groups
adding 4-21
assigning AAA clients or AAA servers to 4-22
configuring 4-20
deleting 4-24
enabling in interface 3-6
overview 1-20
reassigning AAA clients or AAA servers to 4-23
renaming 4-23
network requirements 2-4
network topology 2-5
notifications H-9
Novell NDS user databases
authentication 11-24
configuring 11-28
mappings
database group to a AAA group 12-13
Novell Requestor 11-25
supported databases H-4
supported protocols 1-10
supported versions 11-24

O

ODBC features
accountActions table 8-28
authentication
CHAP 11-34
overview 11-30
PAP 11-33
result codes 11-39
case-sensitive passwords 11-34
CHAP authentication
sample procedure 11-36
configuring 11-41
data source names 11-30
group mappings 12-10
group specification
CHAP 11-39
PAP 11-37
vs. group mapping 12-12
Microsoft SQL Servers
case-sensitive passwords 11-34
Oracle
case-sensitive passwords 11-34
PAP authentication
sample procedures 11-35
stored procedures
CHAP authentication 11-38
implementing 11-33
PAP authentication 11-36

Downloaded from www.Manualslib.com manuals search engine

type definitions 11-34
supported databases H-5
supported protocols 1-10
user databases 11-30
ODBC import definitions G-1
ODBC logs
See logging
Online Documentation
using 1-28
online Help 1-23
operating system requirements 2-3
outbound passwords
configuration 1-12

P

PAP
compared with ARAP 1-11
compared with CHAP 1-11
compatible databases 1-9
in User Setup 7-6
Passed Authentications log
configuring CSV 9-22
CSV file directory 9-10
enabling CSV logging 9-19
frequency 9-10
viewing 9-20
password aging
Cisco IOS release requirement for 6-20
interface configuration 3-5
rules
in Group Setup 6-20
passwords
aging
See password aging
CHAP/MS-CHAP/ARAP 7-8
configurations
caching 1-12
inbound passwords 1-12
outbound passwords 1-12
separate passwords 1-12
single password 1-12
token caching 1-12
token cards 1-12
expiration 6-22
import utility H-5
information
in post-login greeting 6-23
Microsoft SQL servers
case-sensitive 11-34
Oracle
case-sensitive 11-34
protocols and user database compatibility 1-9
protocols supported 1-10
user-changeable 1-14
validation options in System Configuration 8-4
performance monitoring H-7

Downloaded from www.Manualslib.com manuals search engine

per-group attributes
enabling in interface 3-2
per-user attributes
enabling in interface 3-2
TACACS+/RADIUS in Interface Configuration 3-4
PIX ACLs
See downloadable PIX ACLs
PIX command authorization sets
See command authorization sets
PIX Firewalls
troubleshooting A-16
port 2002 H-2
port allocation
See HTTP port allocation
PPP
password aging 6-20
processor utilization H-8
profile components
See shared profile components
protocol options
in user-level TACACS+ settings 7-24
proxy
character strings
defining 4-6
stripping 4-6
configuring 4-25
in enterprise setting 4-6
overview 4-4
sending accounting packets 4-7
troubleshooting A-12
Proxy Distribution Table
adding entries 4-26
configuring 4-25
default entry 4-3, 4-25
deleting entries 4-29
editing entries 4-28
match order sorting 4-28
overview 4-25

Q

quotas
See network access quotas
See usage quotas

R

RADIUS
Accounting log
See RADIUS Account log
attributes
in User Setup 7-36
See also RADIUS VSAs
AV pairs
Ascend D-21
Cisco IOS D-3
IETF D-12
IETF accounting D-16

Downloaded from www.Manualslib.com manuals search engine

IETF vendor-proprietary D-10
overview D-1
See also RADIUS VSAs
Cisco Aironet
in Network Configuration 4-10
IETF
in Group Setup 6-34
interface configuration 3-12
in User Setup 7-37
interface configuration overview 3-10
See also RADIUS VSAs
specifications 1-6
troubleshooting A-18
tunneling packets 4-12
vs. TACACS+ 1-5
RADIUS Accounting log
configuring
CSV 9-20, 9-22
ODBC 9-27
CSV file directory 9-8
enabling
CSV 9-19
ODBC 9-27
RADIUS user databases
configuring 11-50
group mappings 12-10
RADIUS-based group specification 12-21
RADIUS VSAs
Ascend
in Group Setup 6-37
interface configuration 3-14
in User Setup 7-39
Cisco Aironet
in Group Setup 6-16
in User Setup 7-37
Cisco BBSM
in Group Setup 6-45
in User Setup 7-48
supported attributes D-9
Cisco IOS/PIX
in Group Setup 6-36
interface configuration 3-14
in User Setup 7-38
supported attributes D-4
Cisco VPN 3000
in Group Setup 6-38
interface configuration 3-15
in User Setup 7-41
supported attributes D-6
Cisco VPN 5000
in Group Setup 6-39
interface configuration 3-16
in User Setup 7-42
supported attributes D-9
custom
in Group Setup 6-46

Downloaded from www.Manualslib.com manuals search engine

in User Setup 7-49
Juniper
in Group Setup 6-44
interface configuration 3-19, 3-20
in User Setup 7-47
supported attributes D-30
Microsoft
in Group Setup 6-41
interface configuration 3-17
in User Setup 7-44
supported attributes D-18
Nortel
in Group Setup 6-42
interface configuration 3-18
in User Setup 7-45
supported attributes D-29
See also AV pairs
user-defined
about E-27
adding E-28
deleting E-29
import file E-31
listing E-30
replicating E-27
RDBMS synchronization
accountActions table
as a transaction queue 8-28
configuring 8-37
data source name configuration 8-34
disabling 8-39
enabling in interface 3-5
overview 8-24
partners 8-35
report and error handling 8-29
RDBMS Synchronization log
CSV file directory 9-16
overview 9-16
viewing 9-20
README.TXT xxxi
REBOOT.BAT H-10
Registry H-2
rejection mode
general 12-3
Windows NT/2000 user databases 12-4
related documentation xxxi
release notes xxxi
remote access policies 2-13
remote logging
See logging
replication
backups recommended (Caution) 8-12
cascading 8-14
clients
configuring 8-17
components
overwriting (Caution) 8-17
overwriting (Note) 8-13
selecting 8-13

Downloaded from www.Manualslib.com manuals search engine

configuring 8-20
corrupted backups (Caution) 8-12
disabling 8-23
frequency 8-10
important considerations 8-10
in System Configuration 8-20
interface configuration 3-5
logging 8-12
master AAA servers 8-7
messages B-6
notifications 8-23
overview 8-6
partners
configuring 8-22
options 8-15
scheduling 8-20
selecting data 8-13
user-defined RADIUS vendors 8-11
vs. backup 8-11
reports
See also logs
See Disabled Accounts report
See Logged-In Users report
Reports and Activity
configuring 9-23
CSV logs 9-15
in interface 1-23
See also logging
request handling
general 12-3
Windows NT/2000 user databases 12-4
requirements
hardware 2-2
network 2-4
operating system 2-3
system 2-2
third-party software 2-3
resource consumption H-8
RESTART_ALL_SERVICES.BAT H-10
RESTART_PROTOCOL_MODULES.BAT H-10
restarting services 8-2
restore
components restored
configuring 8-47
overview 8-47
filenames 8-45
in System Configuration 8-45
overview 8-45
performing 8-47
reports 8-47
with CSUtil.exe E-6
RFC2138 1-6
RFC2139 1-6
RSA user databases
configuring 11-57
group mappings 12-10

Downloaded from www.Manualslib.com manuals search engine

S

SafeWord user databases
  configuring 11-54
  group mappings 12-10
search order
  external user databases 12-8
security policies 2-14
security protocols
  Cisco AAA client devices 1-2
  CSRadius H-11
  CSTacacs H-11
  interface options 3-9
  RADIUS 1-5
  TACACS+
    custom commands 3-8
    overview 1-5
    time-of-day access 3-8
service control
  in System Configuration 9-35
service logs
  configuring 9-35
Service Monitoring log
  See ACS Service Monitoring log
services
  logs
    configuring 9-35
    list of logs generated 9-34
  management 8-48
  overview H-2
  starting 8-2
  stopping 8-2
session policies
  configuring 10-14
  options 10-13
  overview 10-13
shared profile components
  overview 5-1
  See also command authorization sets
  See also network access restrictions
shared secret H-11
shell command authorization sets
  IETF
    in Group Setup 6-30, 7-26
  See also command authorization sets
single password
  configuration 1-12
SMTP H-9, H-11
space H-8
specifications
  RADIUS
    RFC2138 1-6
    RFC2139 1-6
  system performance 1-3
  TACACS+ 1-6
SQL
  See Microsoft SQL
starting services 8-2

Downloaded from www.Manualslib.com manuals search engine

states H-9
static IP addresses 7-11
stopping services 8-2
stored procedures
  CHAP authentication
    configuring 11-43
    input values 11-38
    output values 11-38
    result codes 11-39
  implementing 11-33
  PAP authentication
    configuring 11-43
    input values 11-36
    output values 11-37
    result codes 11-39
  sample procedures 11-35
  type definitions
    integer 11-34
    string 11-34
supplementary user information
  in User Setup 7-7
  setting 7-7
system configuration 8-1
system health H-7
system messages
  event log B-1
  failed attempts B-9
  in interface 1-23
  replication B-6
  system monitored events B-2
system monitoring
  See monitoring
system requirements 2-2

T

TAC
  accessing xxxiv
  overview xxxiv
TACACS+
  Accounting log
    See TACACS+ Accounting log
  Administration log
    See TACACS+ Administration log
  advanced TACACS+ settings
    in Group Setup 6-2
    in User Setup 7-31
  AV pairs
    accounting C-4
    general C-1
  custom commands 3-8
  enable passwords
    in User Setup 7-34
  enable privilege options 7-32
  in Group Setup 6-28
  interface configuration 3-7
  interface options 3-9

Downloaded from www.Manualslib.com manuals search engine

outbound passwords
in User Setup 7-35
SENDAUTH 1-13
settings
in Group Setup 6-2
in User Setup 7-24
specifications 1-6
time-of-day access 3-8
troubleshooting A-18
vs. RADIUS 1-5
TACACS+ Accounting log
configuring
CSV 9-22
ODBC 9-27
CSV file directory 9-6
enabling
CSV 9-19
ODBC 9-27
viewing 9-20
TACACS+ Administration log
configuring
CSV 9-22
ODBC 9-27
CSV file directory 9-7
enabling
CSV 9-19
ODBC 9-27
viewing 9-20
Technical Assistance Center
See TAC
Telnet
password aging 6-20
test login frequency
internal testing H-10
third-party software requirements 2-3
thread used H-8
time-of-day/day-of-week specification
enabling in interface 3-4
timeout 12-6
TLS
overview 8-71
token caching
password configuration 1-12
token cards
password configuration 1-12
settings in Group Setup 6-17
token servers
ActivCard 11-49
AXENT 11-55
CRYPTOCard 11-49
ISDN terminal adapters 11-48
overview 11-48
RADIUS-enabled 11-49
RADIUS token servers 11-49
RSA 11-56
SafeWord 11-53
supported servers H-4

Downloaded from www.Manualslib.com manuals search engine

token caching 11-48
Vasco 11-49
topology
See network topology
troubleshooting
administration issues A-2
browser issues A-3
Cisco IOS issues A-4
database issues A-5
debug logs 9-34, A-11
dial-in issues A-6
installation issues A-13
max sessions issues A-13
PIX Firewall issues A-16
proxy issues A-12
RADIUS issues A-18
report issues A-14
TACACS+ issues A-18
third-party server issues A-15
upgrade issues A-13
user issues A-16
trust relationships 11-8

U

UNIX passwords H-5
unknown user policies
configuring 12-8
in external user databases 12-8
unknown users
handling method 12-1
network access authorization 12-7
upgrading
troubleshooting A-13
usage quotas
in Group Setup
session-based 6-13
in Interface Configuration 3-5
in User Setup 7-19
overview 1-16
resetting
for groups 6-49
for single users 7-55
user callback options
setting 7-10
user-changeable passwords 1-14
user database options H-4
user data configuration
in Interface Configuration 3-3
user-defined actions H-10
user groups
See groups
user-level
downloadable ACLs
enabling in interface 3-4
network access restrictions
enabling in interface 3-4
See also network access restriction sets

Downloaded from www.Manualslib.com manuals search engine

network access restriction sets
enabling in interface 3-4
See also network access restrictions
users
adding 7-5
assigning client IP addresses to 7-11
assigning to a group 7-9
configuring 7-2
configuring shell command authorization sets for 7-26
customized data fields 3-3
deleting 9-12
deleting accounts 7-54
disabling accounts 7-6
finding 7-52
in multiple databases 12-4
in multiple domains 12-4
listing all users 7-51
number of 2-17
relationship to groups 3-2
saving settings 7-56
supplementary information 7-7
troubleshooting A-16
types
cached 12-2
known 12-2
unknown 12-2
VPDN dialup F-2
User Setup
basic options 7-4
configuring 7-2
deleting user accounts 7-54
saving settings 7-56
Users in Group button
in Group Setup 6-48

V

validation
passwords in System Configuration 8-4
Vasco user databases
group mappings 12-10
RADIUS-based group specification 12-21
vendor-specific attributes
See RADIUS VSAs
virtual private dialup network
See VPDN
Voice-over-IP
See VoIP
VoIP
accounting configuration in Interface Configuration 3-6
Accounting log
See VoIP Accounting log
enabling in interface 3-6
group settings in Interface Configuration 3-6
in Group Setup 6-4
VoIP Accounting log
configuring
CSV 9-22

Downloaded from www.Manualslib.com manuals search engine

ODBC 9-27
CSV file directory 9-9
enabling
CSV 9-19
ODBC 9-27
viewing 9-20
VPDN
advantages 2-11
authentication process F-1
domain authorization F-2
home gateways F-3
IP addresses F-3
tunnel IDs F-3
users F-2
VSAs
See RADIUS VSAs

W

warning events H-8, H-9
watchdog packets
configuring on AAA clients 4-12
configuring on AAA servers 4-16
web servers H-2
Windows 95/98 operating systems
dial-up networking 11-11
domain names 11-11
Windows NT/2000 operating systems
Active Directory 11-12
authentication order 12-5
Cisco Secure ACS-related services
See services
dial-up networking clients
domain field 11-9
password field 11-9
username field 11-9
domains
domain names 11-11, 12-4
mappings 12-17
trusted 11-8, 11-11
environment overview H-2
Event logs H-9
grant dial-in permission to user
in user databases 11-8, 11-13
group mappings
editing 12-17
no access groups 12-15
remapping 12-17
mappings
database group to a AAA group 12-13
Registry H-2
rejection mode 12-4
request handling 12-4
trust relationships 11-8
user databases
configuring 11-13
grant dial-in permission to user 11-8, 11-13
overview 11-6

Downloaded from www.Manualslib.com manuals search engine

passwords 1-10
supported databases H-4
user manager 11-12

Downloaded from www.Manualslib.com manuals search engine